International REVIEW
IPRA CINDER
ISSUE 1
January - June 2017

Blockchain in Public Registries: Don't Expect Too Much
Benito Arruñada

Maintaining the Quality of Information in the Land Title Register: Data Repair Mechanisms
Pamela O'Connor

Blockchains and Title Registration
Luis Gallego

Blockchain Technology: the Last Mile for Electronic Property Registry Systems
Adriana Jacoto Unger, Flavio S. Correa da Silva and João Marcos M. Barguil

What does Blockchain Registry Mean for the Owner?
Teófilo Hurtado Navarro

The Blockchain Cures Cancer (and replaces notaries, etc.)
Matt Regan

The Impact of "Disruptive" IT and the Registrar's Role in Future e-Conveyancing
Jacques Vos

BOOK REVIEW
Das Grundbuch im Europa des 21. Jarhunderts [Land Registry in 21st Century Europe]
Bruno Rodríguez-Rosado

ipra-cinder

INTERNATIONAL PROPERTY REGISTRIES ASSOCIATION

IRIB

Instituto de Registro
Imobiliário do Brasil

ABDRI

ACADEMIA
BRASILEIRA
DE DIREITO
REGISTRAL
IMOBILIÁRIO

Quinta
editorial

International REVIEW
IPRA CINDER
ISSUE 1
January - June 2017

International REVIEW IPRA CINDER
ISSUE 1 January - June 2017

Letter to the reader

This electronic review on Land Registration is an initiative approved at the 20th IPRA-CINDER World Land Registration Congress that took place in Dubai in 2016. A CINDER review did exist in the past, but our expectation is that the new format and language used will allow us to reach a broader audience. Just as Land Registries have evolved since the foundation of our organization 45 years ago, the way knowledge is transmitted, the language used and the topics on the table have changed. The Review is not only for Land Registrars but also researchers, academics, public officials and professionals—anyone dealing with or interested in Land Registration. Our aim is to promote the exchange of ideas between academia and practitioners. IPRA-Cinder has brought together top professors from different legal traditions the world over to compose our scientific committee, and I want to thank each of them.

This edition is divided into three parts. First, an academic article from Professor Pamela O'Connor presents a key issue that currently affects all Land Registries around the world: how to keep information updated. The second section of the edition comprises a debate on new technology that may have great impact in the near future. Here, Professor Arruñada poses some questions about blockchain technologies; Engineer and Land Registrar Luis Gallego explains what exactly a blockchain is and how it relates to Land Registration; two Land Registrars provide views from different registration systems (Jacques Vos, The Netherlands and Teofilo Hurtado, Spain); and from Brazil, Adriana Jacoto Unger, João Marcos M. Barguil and Flávio S. Correa da Silva discuss the topic from the point of view of the Brazilian academic community. The segment concludes with the industry's point of view, presented by Matt Regan. The edition's third section is composed of a book review by Professor Bruno Rodriguez on a recent German publication about Land Registration in Europe. Mr. Rodriguez is also the secretary of this review and has collaborated in its creation.

This review has been entrusted to the IPRA-CINDER South American delegation, based in Sao Paulo, Brazil. Thanks to Sergio Jacomino of the IRIB and his team, this initiative has been made possible and will be published biannually. We greatly value reader opinions and the advice of our scientific committee.

Nicolás Nogueroles
Secretary General, IPRA-CINDER

Table of Contents

6 Blockchain in Public Registries: Don't Expect Too Much
Benito Arruñada

12 Maintaining the Quality of Information in the Land Title Register: Data Repair Mechanisms
Pamela O'Connor

26 Blockchains and Title Registration
Luis Gallego

52 Blockchain Technology: the Last Mile for Electronic Property Registry Systems
Adriana Jacoto Unger, Flavio S. Correa da Silva and João Marcos M. Barguil

56 What does Blockchain Registry Mean for the Owner?
Teófilo Hurtado Navarro

62 The Blockchain Cures Cancer (and replaces notaries, etc.)
Matt Regan

68 The Impact of "Disruptive" IT and the Registrar's Role in Future e-Conveyancing
Jacques Vos

76 BOOK REVIEW
Das Grundbuch im Europa des 21. Jahrhunderts [Land Registry in 21st Century Europe]
Bruno Rodríguez-Rosado

Blockchain in Public Registries: Don’t Expect Too Much

Benito Arruñada, Professor
Pompeu Fabra University and Barcelona GSE, Barcelona (Spain)

Abstract This article aims to determine the importance of blockchain for Land Registries, making a distinction between contract and property rights. There is a tendency for blockchain supporters to overestimate the power of private ordering and to minimize that of trusted intermediaries. Blockchain claims to eliminate intermediaries, but analysis proves the contrary. The author analyzes the impact of blockchain in conveyancing and in property titling, showing that it is easier to expand this technology in the fields of notarization and data archiving than to replace “title by registration” systems. There is also the need to distinguish between deed system and title system when evaluating the impact of blockchain. Property “recordation” and company registries are going to be more affected by blockchain than title registration systems because registration reviews cannot be easily carried out by an automatic system.

Blockchain—often known as “distributed ledger technology”—has been sold as the most important technological innovation in today’s economy. Even if it is difficult to separate substance from hype, not only have thousands of blockchain applications been launched, but the largest firms in many industries are investing substantial amounts of resources in blockchain-related efforts. However, it is also becoming apparent that serious and recurrent difficulties are delaying, if not killing off, what for the time being are still modest applications of the technology.

This article aims to ascertain the importance of blockchain for Land Registry. After introducing the basics of blockchain and smart contracts, it will examine blockchain applications from the perspective of the law-and-economics analysis of property rights, paying particular attention to the legal distinction between contract (personal or *in personam*) rights and property (real or *in rem*) rights, and to the distinction between private and public legal "ordering."

A common problem of blockchain applications is a tendency to overestimate the power of private ordering and to minimize that of trusted intermediaries. This has often led to unmet expectations. While market participants can trade contract rights easily under private ordering arrangements based on reputational assets and the expectation of future trade, trading in *in rem* rights requires a minimum of public ordering—in particular, an enforcer who is neutral and independent not only of parties to a given contract but also to all holders of property rights on the type of asset being traded in that market. These limitations constrain the possibilities of applying blockchain to public contractual registries.

Blockchain and smart contracts

Blockchain is the technology underpinning the Bitcoin cryptocurrency. As with any other type of money, electronic currency must make sure that it changes hands without any risk of being diverted and that it is not spent twice by the same individual. Traditional payment systems solve these problems by relying on central, specialized and trusted third parties such as banks, payment systems, credit card companies and clearing houses. In contrast, the blockchain solves them with a peer-to-peer solution. It is able to replace the trusted third party because it contains the history of all previous transactions, and therefore is a source of evidence for establishing who owns what at any given moment. To do this, it replicates the ledger in a multitude of computers or "nodes", making all the history of transactions public, accessible and widely distributed across the whole network of users.

Blockchain applications have been expanded by embedding information in the ledger, potentially including in it all steps in the contractual process, from ensuring the reliable recording and archiving of data to the transfer of all types of assets. Therefore, blockchain technology is now applicable not only to payments but, allegedly, to all sorts of contracts relying on trust.

It is even said to be "trustless", indicating that it does not need trust to work. However, this trustless feature needs to be qualified. Blockchain and all other institutional and physical technologies supporting impersonal exchange seek to trade trust held by all parties towards a third-party intermediary—a register

or organized exchange, bank, credit card system, etc.—for trust between counterparties. Blockchain enthusiasts claim that it gets rid of intermediaries but this claim proves illusory: this is more a Holy Grail than a realistic objective.

In fact, different types of intermediaries play key roles and their presence holds important consequences for firms' strategy and the structure of contracting.

- First, blockchain applications will tend to rely on dual structures of casual and formal transactions, with the formal stage being highly abstract, using simple contracts and enforcing a closed number of property rights.

- Second, the core peer-to-peer structure of blockchain faces insurmountable difficulties to reach contractual completion and to interact with the real world, two difficulties that must be framed in terms of, respectively, contract (*in personam*) rights and property (*in rem*) rights.

- Third, to overcome these difficulties and to complement its core peer-to-peer structure, blockchain development will encourage the proliferation of a myriad of new specialists to provide, to most end users and for most assets, effective contractual completion as well as interfaces between the virtual and real worlds.

- Fourth, the emergence of specialized agents will reduce total costs at the price of increasing agency costs, therefore creating additional conflicts of interest. This will open up additional opportunities for fraud and trigger greater demand for centralized and specialized enforcement and regulation.

- More generally, because of the role of intermediaries, blockchain is likely to affect transaction costs in all types of transactions, modifying the comparative advantage of different organizational forms and institutions, e.g., the optimal degree of vertical and horizontal integration in business firms and other organizations; and even the relative optimal scope of markets and politics as information, decision and allocation mechanisms. Not only the extent but also the sign of these impacts are open to question. Therefore, contrary to expectations, it is debatable if blockchain really favors market transactions over business firms.

- Lastly, blockchain will find it easier to enable transactions in personal rights as compared to real (i.e., property, *in rem*) rights. To move from the world of personal rights to the world of real rights will require public interfaces and interventions (at the very least, to establish the status of the blockchain as judicial evidence). Therefore, applications

of blockchain in property transactions will likely be limited to document notarization and property conveyancing, as well as, at the most using private blockchains for archiving purposes within standard registration systems.

The following discusses the latter point in greater detail.

Blockchain in conveyancing and creating property titles

The impact of blockchain on conveyancing and creating property titles will be affected by the basic characteristics of both legal processes, which, in line with participant incentives, are mostly private in conveyancing and intrinsically public in registration. In particular, they are defined by the fact that in all property systems, parties are free to choose their lawyers, conveyancers and notaries public. By contrast, third-party protection leads the law to universally restrict their choice of the office that records their titles or the registrar that preserves and reviews their rights, as well as the judge who presides over a suit of quiet title or any equivalent judicial procedure. Therefore, blockchain should find it easier to expand into notarization and data archiving, but will find it more difficult to replace land registries, especially in jurisdictions such as Australia, England, Germany or Spain, which have registries of rights, also often called "land registration" or "title by registration" systems.

First, to the extent that even in civil law jurisdictions public notaries are freely chosen by parties to private contracts, the blockchain will play a bigger role in notarization. The only functions for which notaries used to be clearly superior were in identifying parties and, more clearly, in ascertaining their legal capacity. However, both advantages are threatened by technological developments in identification and the related availability of registries for individuals' legal capacity. Both functions are also substantially affected by blockchain, which has allowed the development of services that provide authentication and authorization, proving to other parties that you are who you say (authentication) and you have the required permissions (authorization).

Second, the applicability of blockchain to registries will be more limited because registries play a public legal function, protecting the interest of unrepresented third parties and therefore being much more than mere public databases. Describing a Land Registry as a ledger is somehow misleading. Land Registries are not standard ledgers. Systems based on the recordation of deeds merely time-stamp and archive documents and are therefore closer to a simple ledger, but the date of entry at the registry holds crucial legal consequences, allowing the record to provide evidence on the priority of legal claims. Registries of rights are even more complex: they provide a sort of legal "balance sheet" defining not mere claims

but the rights on a specific property. The "ledger" terminology focuses on the numeric or accounting aspect while the key element in registries is legal: they do not mainly contain magnitudes (values) but the legal evidence supporting claims (recording) or certifying rights (registration).

In principle, when considering the impact of blockchain for property registries, it is sensible to distinguish between recorders of deeds, such as those of France or the U.S., and registers of rights, such as the German Grundbuch or the Torrens system of title by registration operating in Australia. The latter not only date and keep the documents or "deeds" reflecting the transactions that the contractual parties agree to but also verify, as a necessary condition for entry into the register, that the intended transactions respect all other right holders' rights on the specific asset.

It is conceivable that a deed recordation system might be replaceable with an automatic system of dating private contracts and preserving their contents, providing parties to private contracts cannot manipulate these two functions once they sign their contract. However, even in that case, there is still a need for some public authority to establish the rules of evidence: to set the value of the blockchain as a source of evidence for *in rem* adjudication. To produce *in rem* effect, all parties must be obliged to express their will through the blockchain. Moreover, this authority must trust those designing, putting in place and—to some extent—governing or at least affecting the decentralized government of the blockchain system.

The case of company registries is similar, to the extent that most of them are closer to recordation than to registration systems. However, company registries could be challenged by initiatives like the Ethereum blockchain, which aims to create virtual decentralized and autonomous organizations that would be defined only by a given set of rules running in the blockchain. In principle, such organizations could be flexibly organized, allocating specialized managerial and contractual functions in different manners.

A less ambitious initiative is that of developing an international standard for the identification of legal entities, known as the Register of Legal Organizations (ROLO). It is revealing that, despite being led by collaborative industry, given that most transactions are business-to-business, what is being considered is the need for ROLO in each nation, and the expected presence of a required element.

Another area related to company registration in which blockchain has the potential to automate transactions is that of corporate actions, that is, announcements made by a public company that affect its securities and may require action by either investors or their representative

agents. Examples include dividends and coupon payments, offers to issue or redeem securities, stock splits, mergers and spin-offs. Most of this data is communicated to investors through a complex channel involving suppliers of financial data, securities' custodians and investment fund managers, who then also carry investors' decisions in the opposite direction. In both directions, blockchain could make the whole process much more efficient and automatic.

In comparison with property recordation and company registries, property registries of rights (often called "title systems") are likely to be less affected by blockchain, because registration review cannot be easily exercised by an automatic system. Even greater difficulties would be entailed than those considered above with respect to contractual completion.

The *White Paper* of a 2016 Swedish inter-agency initiative provides a valuable illustration as, in essence, it is limited to reorganizing the *in personam* contractual process that precedes the *in rem* property transaction. The changes proposed in Sweden thus resemble the "Landonline" system of electronic conveyancing and registration implemented in New Zealand since 2009, but with the Land Registry retaining, at least initially, all its powers to review and decide on registration. The Register would also define the assets and (supposedly) the authority to deal. Therefore, the only substantial novelty proposed by the *White Paper* is that it relies on blockchain for the electronic conveyancing application.

This work contains revised excerpts of the author's paper "Blockchain's Struggle to Deliver Impersonal Exchange", available at https://ssrn.com/abstract=2903857.

Maintaining the Quality of Information in the Land Title Register: Data Repair Mechanisms

Pamela O'Connor, Professor
University of the Sunshine Coast Law School (Australia)

Abstract The accuracy of the Land Registry and keeping the information up to date is essential for the performance of the system. This article poses three main problems that affect this accuracy. First, unregistered transfers or transactions. There are different reasons why this occurs. The author asks if the legal rule that requires registration is enough incentive to register. Encouraging parties to register is a regulatory problem. Is adverse possession inconsistent with a title registration system? This article offers a singular view on the question. Second, changes in occupational boundaries. How do boundaries change? A legal rule is needed to adjust occupational boundaries with the boundaries recorded in the register. Third, registry errors are challenging the integrity and accuracy. How can the errors be corrected? How to allocate liability? And in the end, who gets the land and who gets monetary compensation? These are key questions.

1. INTRODUCTION

Land title registers serve multiple objects. They support the development and operation of land markets. They also provide the foundation for broader land administration functions and land information systems. All the objects are better served if the data is kept accurate, complete and up to date. This article examines three sets of challenges which arise in maintaining title registers, and considers the implications for the design of the system's legal rules.

The first set of challenges arises from unregistered transfers and transactions. To keep property data up to date, registries rely on transacting parties to notify them of changes by lodging documents (or electronic data) for registration. In all systems, some property transactions take place informally, without notification to the registry, and therefore go unrecorded. The passing of ownership by inheritance is a common cause of unrecorded changes, but property transactions occur off-register for a variety of reasons. A multi-faceted regulatory response is needed to ensure that people can and do register their dealings. In addition, a legal mechanism is needed to re-establish the ownership data in a parcel record after the chain of registered dealings has been broken by an off-register transfer.

Changes to occupational boundaries give rise to a second set of challenges. The boundaries of a registered parcel are defined by reference to cadastral survey or, in some countries, by 'general boundaries' aligned to topographic features. The boundary of a parcel as actually occupied can deviate from the cadastral boundaries due to long-standing and unchallenged encroachment by neighbours. In many cases, no fault lies with the neighbour presently occupying the area of land which is the subject of the encroachment. A discrepancy between the registered land description and the occupational boundaries is a trap for purchasers, because small but significant differences in measurement are difficult to detect without a re-survey. A legal rule is needed to reconcile the occupational boundaries with the boundaries recorded in the register, either by amending the register or by ending the encroachment.

The third set of challenges arises from errors in registered data. A registration error occurs when, due to a failure by the registry, a register entry is made which should not have been made, or an entry which should have been made is omitted.[1] The categories of error range from a slip of little consequence to an error which creates or destroys a property right. Since the making of an error or its correction can cause somebody loss, difficult questions arise about whether an error should be corrected and how losses should be allocated.

2. THE PROBLEM OF INFORMAL TRANSACTIONS

2.1 Limited effect of incentives to register changes in ownership

A key issue for the design of registered title systems is whether to recognize particular types of property right as capable of existing without registration. For present purposes, a property right is a right *in rem*, meaning a right held in the land which the holder can enforce against anyone who deals with the land. Because

[1] *Errors resulting from fraud or for which a lodging party is responsible are excluded from this discussion.*

it may not be efficient or practical to require registration of all *in rem* rights, the systems usually exempt a few specified classes. Once created, these 'overriding interests' are enforceable against registered owners under the statutes.

Apart from a restricted class of overriding interests, the general rule in registered title systems is that registration is required to complete the transfer of ownership or the creation of lesser interests such as charges and servitudes. In other words, registration is necessary to constitute certain types of *in rem* rights.

A legal rule requiring registration to constitute an *in rem* right serves a dual function. First, it gives the acquirers of interests an incentive to register their interests. Second, it limits the information costs of purchasers. In theory, purchasers can omit searching beyond the register for claims that will not be enforceable against them once they obtain registered title.

In practice, the incentive to register a dealing is not always sufficient to ensure that the registry is notified of changes in ownership. Acquirers of interests may not anticipate a future need to call on the law to assist in enforcing their rights, or may not need to use the formal transfer or credit systems. There may be factors which act as disincentives to registration of dealings. Registration entails costs, including the drafting, execution and lodgement of documents, property taxes and lodgement fees.

In 2007, Barnes and Griffith-Charles reported on the findings of their investigation into the reversion of formal registered land titles to the informal system in St Lucia.[2] After 15 years, 28% of the registered titles in their sample of 60 were in the name of deceased persons, and the land was currently held by a relative claiming through inheritance.[3] In their investigation of the causes of non-registration, they found that landholders generally overestimate the costs of registration and underestimate the benefit of the legal security it provides.[4]

Encouraging transacting parties to register dealings is a regulatory problem. There are many factors which influence behaviour for and against formalization, and some are difficult for regulators to control. Factors which can influence registration behaviour include the actual and perceived costs of registration; delays or inefficiencies in registry processing; the financing of transactions by institutional lenders who require registered security interests; the existence of planning controls on unregulated subdivision; the use of professionals such as lawyers to complete land transactions;

[2] *G Barnes and C Griffith-Charles, 'Assessing the formal land market and deformalization of property in St Lucia' (2007) 24 Land Use Policy 494.*

[3] *Ibid 499.*

[4] *Ibid 499-500*

the persistence of traditional modes of transacting, the desire of acquirers to avoid publicity for their landholdings, and cultural factors.

One informal transaction is likely to be followed by others.[5] Land titles descend or devolve through a chain of transfers from one registered owner to another, each formalized by a register entry. Once the chain is broken by an off-register dealing, a landholder who enjoys only informal title can pass no formal title to a successor. Any subsequent transactions will also take place off-register.

Each successive landholder enjoys many of the benefits of ownership, but is unable to use the land as collateral to obtain formal credit. The land cannot do its work in aiding capital formation, and is likely to remain undeveloped and undervalued. Where a number of parcels in an area are held under informal tenure, the area may suffer the effects of under-investment.

The reversion of parcels from the formal (registered) system to informal tenure frustrates the objects of title registration. The existence of a landholder with de facto tenure raises transaction costs, as a purchaser must consider the landholder's claim and the enforcement costs. The discrepancy between the registered title and the de facto tenure devalues the parcel record in the land information system. As Barnes and Griffith-Charles caution: 'if transactions are not registered the registry information will increasingly become out of date until at some point it becomes an historical "snapshot" and not an accurate record of the current tenure situation.[6]'

2.2 A legal rule to return parcels to the formal system

A parcel which has been transferred off-register will continue its parallel transaction history in the informal transfer system until deliberate action is taken to realign the registered title with the informal ownership. In many cases, it would be impractical to retrospectively record a series of dealings that were originally completed off-register. Re-establishment of the register must start with the current reality of who is in possession of the land.

Many legal systems have a rule of acquisitive prescription which under certain circumstances recognizes possession of land for a specified period as a source of original title.[7] In the civil law rule of *usucapio*, the claimant must have acquired possession in good faith and have exercised peaceful and uninterrupted possession.[8] Common law systems have a rule of adverse possession,

[5] *Ibid.*

[6] *Ibid 499.*

[7] *Alejandro Garro, 'Ch 8: Recordation of Interests in Land' in R David et al (ed)* International Encyclopedia of Comparative Law *(Martinus Nihoff Publishers, 2004), [8-83].*

[8] *Barry Nicholas,* An Introduction to Roman Law *(Oxford University Press, 1962) 122.*

which holds that a person in possession of land on his or her own behalf (a 'squatter') acquires a possessory title. Acquisition of possession in good faith is not required at common law, although some statutes require it.[9] The owner of the land has a right to recover possession of the land from the squatter, but has to do so within a limited time period, typically 10-15 years. Once the limitation period has expired, the owner's title is extinguished, leaving the squatter with a better title than anyone else. Many title registration systems allow the squatter to register such a title.

In unregistered land transfer systems, and in deeds registration systems, a rule of adverse possession reduces transaction costs by purging stale claims. A rule which recognizes possession is not inconsistent with an evidentiary system in which deeds are registered as claims. The use of the rule is more controversial in a system of registered title in which registration constitutes a property right and the register provides authoritative ownership data. Registered title is derivative, descending through a line of registered transfers from one owner to another. In a formal sense, it is inconsistent with the authoritative system to recognize title acquired by possession.[10]

There are different schools of thought on whether a registered title system should recognize claims based on adverse possession. Simpson observed the variation in approach from one jurisdiction to another, and even within a jurisdiction over time.[11] Some of the statutes have been amended to allow possessory claims against registered owners at one time, and to disallow it at another time.[12]

The variety of approaches reflects an underlying policy tension. A rule that refuses to recognize long-held possession encourages reversion to the informal transfer system and undermines the marketability of land. On the other hand, a rule that recognizes claims by adverse possession provides incentives for squatters to take possession of land, particularly in common law systems which generally do not require that possession was taken in good faith or under a claim of right. Each jurisdiction makes its own trade-off between the competing policy considerations at a given point in time.

The experience of the Australasian colonies provides a case study of how changed circumstances can lead to change in the rules relating to adverse possession. When the Torrens system was first introduced in the mid-19th

[9] *S Jourdan, Adverse Possession (London, LexisNexis, 2003), 3.24.*

[10] *Lynden Griggs, 'Possessory Titles in a System of Title by Registration' (1999) 21 Adelaide Law Review 157.*

[11] *S R Simpson,* Land Law and Registration *(Cambridge University Press, 1976), 152-53.*

[12] *Ibid.*

century, the early statutes failed to provide a clear rule about adverse possession. When the omission became apparent, some jurisdictions amended their statutes to exclude the application of limitation statutes to registered titles.[13] As time passed, title registrars discovered an increasing number of registered parcels in the names of deceased or missing owners. All Australian States and New Zealand experienced local mining booms which led to an influx of people and subsequent depopulation. Abandonment of land was known to occur in areas where the land market had collapsed following the end of a mining boom.[14] Some cases of apparent abandonment may have been informal transfers. Other causes of missing owners were that a deceased estate had not been administered, or the executors failed to identify the parcel as belonging to the estate.

Many parcels with missing registered owners were occupied by others, who in turn passed their possessory titles to others by transfer and inheritance. In some cases, the 'squatter' in possession of land could trace a derivative title back to the last registered owner through informal transfers, but had no means of proving a claim by registrable documents. A rule was needed to restore the parcels to the formal system. The result is that all Australian states now allow a squatter to apply to be registered as owner of a registered parcel after the previous registered owner's right to sue for recovery of the land has been extinguished by the running of the limitation period.

2.3 Designing a rule

A rule allowing an application to register a title acquired by adverse possession is not necessarily inconsistent with the objects of the title registration system.[15] It depends on the design of the rule. One version provides for extinguishment of the registered title once the limitation period has run, without any adjudication by a competent authority, notification to the registry, or alteration of the title data.[16] This leaves a squatter with the best title, even though the register retains the expired title in its ownership data. It is only through the proof of claim submitted by the squatter that the register can be updated.

The resulting discrepancy in title undermines the principle of public faith in the register. To make matters

[13] *Eg, South Australia, New South Wales and Victoria: ibid 154. See generally, P O'Connor, 'The Private Taking of Land: Adverse Possession, Encroachment by Buildings and Improvement Under a Mistake' (2006) 33 University of Western Australia Law Review 31, 35–38.*

[14] *Simpson, above n 11, 154.*

[15] *Simpson observes that 'it is difficult to understand why it was ever supposed that registration of title had a special quality which somehow made it unnecessary to protect established possession': ibid 152–53.*

[16] *This is the traditional approach of limitation of actions statutes in common law jurisdictions. See eg, Limitation of Actions Act 1954 (Vic) ss 8, 18.*

worse, the squatter's incentive to apply for registration is weak, since nobody can show a better title. Therefore the discrepancy will tend to persist until the squatter needs to deal with his or her title in the formal system.

The squatter's incentive to apply is stronger if registered title can be extinguished only by an order to amend the register made on the squatter's application. Some jurisdictions combine adjudication with a 'veto' rule of adverse possession.[17] The rule allows the registered owner to object to the application, and effectively to veto it.[18] A registered owner who has been dispossessed by the squatter or was unaware of the squatter's occupation can be expected to exercise the veto. An order is likely to be made only in cases where the registered owner is deceased or missing or has abandoned the land. This is just the sort of case where adverse possession law is needed to update the register and restore the marketability of land.

Under a veto rule, the discrepancy between the register and the squatter's de facto tenure will tend to persist so long as the registered owner exercises the right of veto. In 2002, England adopted a conditional form of the veto rule which provides that if a registered owner exercises a veto and fails to recover possession of the land within two years, he or she cannot veto a second application by the squatter.[19] The effect is to set a time limit for resolving the discrepancy between the registered title and the de facto tenure situation. The incentive operates upon the registered owner rather than the squatter.

3. CHANGES IN OCCUPATIONAL BOUNDARIES

3.1. Why occupational boundaries change

One of the major benefits of registered title systems is clear and consistent land descriptions. Parcels are registered with either fixed or general boundaries. In a system which uses fixed boundaries, the parcel is described by reference to a plan of survey which is lodged in the registry. Where general boundaries are used, registered parcels are described by reference to topographical maps which depict permanent physical features such as hedges, fences and roads.[20] While there are presumptions about where the boundary lies in relation to such features, the exact line of the boundary is left undefined when the parcel is registered.[21]

[17] *The rule is named and described in Malcolm Park, 'The Effect of Adverse Possession on Part of a Registered Title Land Parcel' (University of Melbourne, PhD thesis, 2003), 6.3.2.*

[18] *The original veto rule was introduced in South Australia, and later adopted by New Zealand and Queensland, although Queensland repealed its provision.*

[19] *Land Registration Act 2002 (UK) s 96 and sch 6.*

[20] *Simpson, above n11, 127. Systems using general boundaries include England and Wales, Scotland and Cayman Islands.*

[21] *See, eg, Land Registration Act (2002) s 60 and Land Registration Rules (2003) No 1417, Part 10.*

The boundaries of a parcel as actually occupied at a point in time can diverge from the fixed or general boundaries in the registered land description. One possible cause is human behaviour after the parcel is described and registered. A dividing fence or wall may diverge from the line of the cadastral boundary due to an error by an occupier or a contractor, or a mutual mistake by occupiers of both adjoining parcels. Errors in measurement can occur where fences and walls are built without a re-establishment survey. In some cases an occupier may knowingly position a fence off the cadastral boundary to avoid a topographic obstacle such as a tree, possibly with the neighbour's consent. Or a landowner may act unilaterally with the intention of annexing part of a neighbour's land. In many cases, the original cause of a divergence is unknown or forgotten due to the passage of time and subsequent changes of ownership.

Where the boundary of a parcel as actually occupied (the 'occupational boundary') diverges from the boundary in the registered land description (the 'cadastral boundary'), two adjoining parcels are affected. Where a portion of Parcel A is enclosed with and occupied as part of Parcel B, the owner of Parcel B has possession of the portion without title, and the owner of Parcel B has title without possession.[22]

Such discrepancies are common in many countries. Even small differences in measurement can affect the development potential, value and marketability of parcels in closely settled areas. Problems arise because the discrepancy is very difficult for an owner or purchaser to detect by visual inspection without incurring the cost of a re-establishment survey. Purchasers may believe they are acquiring the land as enclosed and occupied by the encroaching owner, although the contract and transfer documents identify the land by its registered land description.

3.2. Rule options

Common law jurisdictions generally use one of three rules.[23] The first is a 'prohibition rule:[24] no adjustment of the location of the boundary is permitted by reason of change in possession or occupation after the parcel is registered. So the adjacent owner is entitled at any time to recover possession of the portion from the encroaching owner. The second is an 'adverse possession rule' which allows the encroaching owner to acquire registered

[22] *The terms are borrowed from Australian encroachment legislation, eg, Property Law Act 1974 (Qld) s 182.*

[23] *Pamela O'Connor, 'An Adjudication Rule for Encroachment Disputes: Adverse Possession or Building Encroachment Statute?' in E Cooke (ed),* Modern Studies in Property Law *Vol 4 (Hart, Oxford, 2007), 197, at 201-14.*

[24] *Park, above n 39, ch 3.5*

title to the portion by adverse possession, and an adjustment of boundaries, once the limitation period has expired. The third approach is a 'building encroachment' statute, which gives a court discretionary powers to determine a just outcome in the circumstances of each case.

3.2.1. No adjustment of boundaries —the prohibition rule

Some jurisdictions prohibit adverse possession claims to registered land generally, while others prohibit or substantially restrict claims to part parcels adjacent to a boundary. The effect is that the cadastral boundaries incorporated into the registered land description are not affected by changes in occupation of the parcels. This 'prohibition rule' promotes certainty and upholds the authoritative nature of registered data. Any discrepancy between the register and occupation is resolved in favor of the cadastral boundaries.

Despite the clarity of the rule, the discrepancy will persist if the adjoining owner fails to take enforcement action to end the encroachment. The failure to act may be due to ignorance of the existence of the encroachment or the circumstances in which it arose, unwillingness to upset the encroaching owner, or the cost of enforcement action.

The prohibition rule imposes costs upon a purchaser, who must avoid boundary errors by discovering if there is a discrepancy. Otherwise, the purchaser bears a dual risk. The first is that a portion of the land transferred may be under encroachment by a neighbour, and the purchaser will incur enforcement costs in recovering possession. The second risk is that the vendor is in possession of a portion of land which the adjoining owner may recover from the purchaser after transfer. The only way to have certainty is to have the land re-surveyed, which adds to the transaction costs.

3.2.2. Adjustment of boundaries by an adverse possession rule

Under a simple adverse possession rule, the adjoining owner retains title to the portion and can sue to recover it, but only until the limitation period expires. If the rule provides that the adjoining owner's title to the portion is extinguished automatically on that date, the problem caused by the discrepancy is worse. The registered land description continues to show the adjoining owner's parcel as including the portion of land, even though the adjoining owner has lost both possession and title. The register is now

seriously at odds with reality, and presents a hazard for purchasers. The discrepancy is likely to continue, because the encroaching owner, who now has the best title to the portion, has a weak incentive to apply for an order to amend the register.

The incentive to update the register is better when a statute provides that the adjoining owner's title to the portion is not extinguished automatically when the limitation period expires, but only by an order to amend the register. Under this rule, the encroaching owner acquires title to the portion only by obtaining the order that will end the discrepancy.

3.2.3. A building encroachment statute

The third approach is a building encroachment statute, which allows for discretionary adjustment of property rights in cases in which buildings encroach across a boundary. These schemes exist in New Zealand, five Australian jurisdictions and three Canadian provinces.[25] The statutes apply in cases where a building, footing or overhang straddles the cadastral boundary and encroaches upon a portion of adjacent land. These are precisely the cases in which bargaining costs are likely to be high. The encroaching owner's investment in the building is a sunk cost which inflates his or her valuation of the portion. The sunk cost represents a 'quasi-rent' which the adjoining owner may try to extract by holding out for an inflated price.[26] The general purpose of the statutes in allowing adjustment of boundaries is to control rent-seeking claims by landowners seeking to make a profit from encroachments, particularly ones that result from human error.[27]

The statutes generally allow either the adjoining owner or the encroaching owner to apply to a court to resolve an encroachment dispute. The court is empowered to make a range of orders to achieve a just outcome. Usually the court can order the removal of the encroaching building, or order the adjoining owner to grant the encroaching owner a transfer, easement or some other right in the portion, and can order the payment of compensation. The statutes allow a court to consider a range of relevant matters including the nature and extent of the encroachment, the loss and damage caused by the encroachment and by its removal, and the circumstances in which the encroachment commenced.

Building encroachment statutes are intended to overcome obstacles to bargaining arising in a context of monopsony (the existence of only one buyer and one seller in the market for the portion). They provide individualized

[25] See Pamela O'Connor, 'The Private Taking of Land' (2007) 33 University of Western Australia Law Review 31, at 54.

[26] TJ Miceli and CF Sirmans, 'An Economic Theory of Adverse Possession' (1995) 15 International Review of Law & Economics 161, 163.

[27] See O'Connor, 'The Private Taking of Land', above n 25, 58–59.

justice based on an ex post facto assessment of the facts. Any order made under the statutes will end the discrepancy by either removing the encroachment or formalizing it on the register.

The statutes are normally used in conjunction with a prohibition rule, and operate as a limited exception. This means that they provide the only means of adjusting registered boundaries to accord with occupation. They do not apply in cases where an encroaching owner has possession of a portion of an adjacent parcel but has not built on it. The use of a prohibition rule in these cases is consistent with a view that the law should not provide for non-consensual adjustment of boundaries where there is no sunk cost or disproportionate loss to impede bargaining between the parties.

4. REGISTRY ERRORS AND CORRECTIONS

The third set of challenges to the integrity and accuracy of the data in the register arises from the existence of errors in the recorded data. Errors may arise on first registration of a parcel, in the survey or land description or in the recording of interests. They can also occur in recording or failing to record subsequent transactions and events. In many cases, errors are not detected for some time, and third parties may have transacted in reliance on the erroneous data.

Correction of erroneous data raises particular difficulty in a system of registered title. The register is an authoritative public record of interests in defined land parcels owned by particular persons at a point in time. In principle, errors in the recording of interests and land descriptions should be corrected to ensure the accuracy of the register and avoid a loss to an innocent party.

Take, for example, a case in which Albert, the owner of a parcel of land ('Greenlands'), subdivides the parcel, and has the registry issue to him two new titles for the subdivided parcels ('Redlands' and 'Whitelands'). Through registry error, an encumbrance which was registered for Greenacre prior to subdivision is omitted when new registered titles are issued for Redlands and Whitelands. The error deprives the encumbrancer of the benefit of a registered encumbrance and represents a windfall gain to Albert, the first registered owner of the two new parcels. So long as Albert remains the registered owner, principle demands that the error should be corrected and the encumbrance registered for both parcels. Although the correction will deprive Albert of the benefit of an unencumbered title, policy does not require that he be compensated for the loss of his windfall gain.

We can now vary the facts to consider a case in which the registry error is first

discovered after Albert has sold Redlands to Bertha. Bertha has purchased Redlands in reliance on the register, which shows the parcel as free of the encumbrance. If the register is to be corrected to restore the encumbrance, Bertha will suffer a loss of part of the value of Redlands. If the register is not corrected, the encumbrancer suffers a loss of a property right in the land. Both Bertha and the encumbrancer are innocent of any fault in causing the error, but only one can have their claim reflected in the register. The encumbrance must be either registered for Redlands, or not. In that sense, only one party can 'get the land'. The other will at best get monetary compensation.

The rules of registered title systems determine who gets the land and who gets the money. Garro finds that the systems usually give priority to the principle of public faith, which protect the purchaser's reliance on the presence or the absence of a registered interest or encumbrance.[28] If Bertha's expectation of obtaining an unencumbered title is defeated by a correction, she will suffer detriment through her reliance on the register. Therefore most systems leave the register uncorrected. The encumbrancer's loss is answered only by monetary compensation.

The systems have different ways of allocating the liability to pay compensation for uncorrected errors caused by a failure of the registry. There may be a public contributory fund to cover losses, or the government may act as the insurer, or the registry may be primarily liable and transfer its risk to a private insurer. Systems based on the Torrens model generally provide that losses caused by registry errors may be compensated from a public insurance fund or by a claim against the State or the registrar as nominal defendant.

Similar principles apply where the registry error is in the land description (including the survey data on which the description is based). The Torrens statutes originally provided for errors in land description to be corrected without reference to the protection of purchasers. The courts read the correction of error provisions subject to other provisions which protect the principle of public faith. The result is that in many Torrens jurisdictions, purchasers for value and all their successors are protected against amendment of parcels due to errors in land description. The errors can be corrected only so long as the land is owned by the applicant for registration of the parcel, or by a person who derives title from the applicant other than for value. The window of opportunity for correcting an error in land description is narrow, and many errors go uncorrected.

5. CONCLUSION

Recent decades have seen title registers established in many countries, to

[28] *Garro, above n 7, [8-148].*

serve economic, social, governance and administrative objectives. The achievement of the objects requires that the information in the register is complete, accurate up to date, so that government and private parties can rely upon it in their decision making and transactions. The causes of informal transactions, changes in occupational boundaries and registry errors are complex, and need to be managed by a range of regulatory interventions operating at many levels.

Where a persistent and serious discrepancy between the registry data and the de facto tenure situation has arisen, it has the potential to undermine reliance on the register and raise transaction costs. If a significant proportion of registered parcels are affected by discrepancies, the achievement of the system's objects may be compromised.

To enable the maintenance of data integrity, the system's legal rules need to provide appropriate mechanisms for repair. Rules are be needed to enable the registry data to be amended to reflect the possession and occupation of land and the intended effect of documents lodged with the registry.

The rules must ensure that correction of registry errors does not undermine the principle of public faith by causing loss to anyone who has relied upon the register. Where a third party acquirer has relied upon the incorrect record, a subsequent correction may cause the acquirer loss. Any other party who suffers loss due to an error that cannot be corrected should, in principle, receive monetary compensation.

Blockchains and Title Registration

Luis Gallego, Director of IT Systems
Colegio de Registradores, Madrid (Spain)

1. Introduction

Block Chains and Records of Rights

At the end of October 2008, in the middle of the financial crisis, Satoshi Nakamoto[1] published, through the Cryptography Mailing List (cryptography@metzdowd.com)[2] and the page: http://www.bitcoin.org,[3] his article: "Bitcoin: A Peer-to-Peer Electronic Cash System", in which the author presented his design for an electronic payment system without trusted third parties: the Bitcoin system. Subsequently, in 2009, he would also publish the first version of the first Bitcoin client program.

Bitcoin[4] is characterized by privacy, its essentially decentralized nature, the absence of a central controlling authority, and the extensive use of cryptography as a means of securing transactions. These characteristics, together with the reaction and distrust that arose in the

[1] *Much has been speculated about the true identity or identities that are hidden under the pseudonym of Satoshi Nakamoto. In May of this year (2015) one of the most promising announcements on this subject occurred when Australian computer scientist Craig Wright, after several previous leaks by third parties, claimed to be said person presenting a series of tests of his authorship, that nevertheless were questioned by some experts. Craig Wright then promised to broadcast the final test, which would consist of transferring bitcoins from one of the initial transaction blocks, something that the true founder could only do with his private key. Finally, however, he would end up recreating, alleging the media and police harassment that, in his opinion, was being submitted, which maintains the question about the authorship of the Bitcoin system.*

[2] *Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,(octubre de 2008). http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html*

[3] *https://bitcoin.org/bitcoin.pdf*

[4] *In the rest of this document, when the term bitcoin appears as: Bitcoin, with the initial letter in capital, reference will be made to the Bitcoin network or system, and to the currency otherwise, just as when using the acronyms BTC.*

face of the central and private banks during the crisis of 2008, explain the exponential development that this cryptocurrency has experienced since its inception.

At the date when this article is written, the bitcoin market[5] is worth more than fourteen thousand five hundred million dollars, with over sixteen million bitcoins in circulation, each with an average market value of around US$ 893.

At present, many companies accept payment for their products or services in bitcoins (WordPress, Microsoft, Virgin, Dell, etc.) or their purchase and exchange in real currencies (Bitstamp,[6] Coinbase,[7] Kraken,[8] Bitfinex,[9] BTC-e,[10] LocalBitcoins,[11] OKCoin,[12] etc.). In addition, new virtual currencies (Litecoin,[13] Ripple,[14] Primecoin,[15] Dogecoin,[16] Zcash,[17] etc.) have begun to emerge following the wake of bitcoin using the same basic technology: block chains.

They are, in fact, chains of blocks, the technological base upon which the success of Bitcoin is based. Indeed, such block chains are a combination of different technologies (Peer-to-Peer networks, asymmetric cryptography, etc.) that have been known for some time. What is truly new is how they have all combined.

The technology has enjoyed such success and attention from the media that new fields have been sought out and identified in which blockchain may be applied. Real estate contracting is among these fields, based on the argument that a block chain system will assure greater security and transparency as compared to current systems, in addition to cost savings that could be adopted in the field by allowing for the elimination of intermediaries who have traditionally been involved in this sector.

This article will analyze these claims in relation to property registry and, more specifically, in relation to the registry of rights, such as in the Spanish Real Estate Registry. But first I will discuss the operation of block chains by studying their implementation in the Bitcoin system.

---

[5] *https://blockchain.info/es/charts*

[6] *https://www.bitstamp.net*

[7] *https://www.coinbase.com*

[8] *https://www.kraken.com*

[9] *https://www.bitfinex.com*

[10] *https://btc-e.com*

[11] *https://localbitcoins.com*

[12] *https://www.okcoin.com*

[13] *https://litecoin.org*

[14] *https://ripple.com*

[15] *http://primecoin.io*

[16] *http://dogecoin.com*

[17] *https://z.cash*

2. Block Chain Function: Bitcoin

2.1. First steps

Bitcoin seeks to implement a secure system to carry out transactions without intervention by a trusted third party (such as a bank). It therefore seeks to establish a system through which monetary transfers can be made and to operate safely even if its users do not know or trust each other. One result, and unlike the traditional banking system, is that in the event of a problem, there is no person, entity or corporation to raise the timely claim, but only users who do not know each other, so no one will be able to answer for the error.

In simplified terms, to achieve the above objective, a digital file is established in which all the transactions carried out between said users are recorded, as an accounting book. A copy of this file is maintained on each of the computers that connect to the Bitcoin network. Therefore, any user can know the transactions made by others.

It is precisely this degree of complete distribution of information that characterizes the Bitcoin system and the blockchain technology that underpins it. No network node, by itself, is decisive or essential for the proper functioning of the system. If any of these nodes is lost, it does not imply loss of information, since all have a complete copy of it, and therefore theoretically no individual or entity could take control of the system.

In Bitcoin, there are different types of nodes or, in other words, nodes that perform different functions:

– First, nodes that only issue transactions (broadcast node): These are wallet applications that only allow for sending or receiving coins through the Bitcoin network. There are applications for all types of devices and also web platforms that offer this service.

– Nodes that propagate transactions (relay node): Their function is mainly to receive transactions and retransmit them to other nodes, but also to verify that they are in the correct format, that the cryptographic signatures they contain are valid and also to verify, in the chain of blocks, that the money transferred exists in the account of origin of the transaction.

– And, finally, nodes that emit, transmit and mine transactions (mining node): In addition to being able to perform the same tasks as the previous types of nodes, their main task is to validate and add the transactions to the block chain as described below.

The nodes of the first group (broadcast node) are the simplest and require less computational capacity, while the latter are the most complex, usually requiring specific hardware to perform the mining tasks at the highest possible speed and which are also essential to ensure the safety of the system.

In simple terms, transferring bitcoins to another user requires nothing more than to relay a message on the Bitcoin network indicating the amount to be transferred and the recipient. With each of these transactions a series of verification operations are performed and, once passed, the accounting file copy of the node that has been verified and other nodes are annotated, in such a way that the transaction book is maintained by all users.

To start operating in the Bitcoin network, the first thing to do is to create one's own wallet in which to store the virtual currencies and that also allow for carrying out transactions. As stated, there are numerous web pages and apps where these wallets may be created. There are many programs to choose from, for all types of devices (personal computers, mobile devices, etc.) or operating systems. It is even possible to find libraries to program our own client program.[18] One of the most popular client applications is BitcoinCore.[19]

Once the application is installed, the client unloads the entire block chain, thus making his/her device into an additional node of the Bitcoin network, in which a copy of the block chain will be stored and subsequently updated.

Currently, the entire block chain occupies approximately 100 Gb. The first time the installed client program is executed, it will download, construct indexes and validate the entirety of the existing block chain at that time which, due to its volume may take several days depending on the speed of the connection and the processing capacity of the device. Once completed, this downloaded copy of the block chain will automatically synchronize itself.

There are also light clients (MultiBit,[20] Electrum,[21] etc.) who only download the headers from the blocks available in the chain, which reduces the downloading and processing times. At the same time, this version is sufficient to determine if a transaction belongs or not to a block without needing to download the complete string.

As mentioned earlier, carrying out transactions involves simply sending a message to the Bitcoin network using the client application and indicating the sender, the recipient and the quantity of bitcoins to be transferred. To ensure that the message is authentic and complete, that is, to prove the identity of the sender and that the message sent has not been modified, electronic signature techniques are used using asymmetric cryptography or two-key cryptography.

To do this, the client applications generate pairs of cryptographic keys, each of which is composed by a public key and a private key. The keys are not independent, but mathematically linked. Public keys are alphanumeric strings of 26 to 35 characters beginning with a '1' or a '3'. An example of a public key would be: 1Hg7wA7JMuMtpXbPMLi6XXh1XwrKK4fwUC. The corresponding private key corresponding

[18] *A list of the possibilities can be seen here: https://es.bitcoin.it/wiki/Software7 https://www.coinbase.com*

[19] *https://bitcoin.org/es/descargar*

[20] *https://multibit.org*

[21] *https://electrum.org*

to it would be: 5J1D73SKtkgjtBGUKPL6EASDb GCKJ226prTAPmnhkyByvpU5deC.

If the client application used is implemented correctly, the cryptographic methods used guarantee that each pair of keys can only be generated once, so it can be assumed that it is impossible for two people to have the same pair of keys. On the other hand, a single person may have more than one pair of keys, which can be useful, for example, to separate and distinguish between virtual currencies with different origins and purposes.

The private key must be kept secret, can be considered as the client's personal signature, allows him/her to encrypt and electronically sign messages sent to the Bitcoin network and is the only way to access and manage the virtual currencies associated with it. Therefore, loss of the key implies the definitive loss of these coins and, likewise, if a third party makes use of our private key, he may dispose of our bitcoins as he wishes.

The public key, on the other hand, can be released freely. It is the only means allowing the user to decrypt messages encrypted or signed with the private key associated with it but, in addition, in the Bitcoin protocol, is how a user is identified,[22] acting somewhat like a user name or e-mail address.

When using the client application to make a bitcoin transfer to another user, the public key for this user must be entered in the recipient field. If the user's public key is entered incorrectly (for example, if a user is specified other than the one to whom we want to send the transfer), and since Bitcoin transactions are irreversible—once they are made, they cannot be reversed—the amount transferred will be lost.

Therefore, great care must be taken to avoid coin losses for any of the reasons stated above—in both the custody of private keys and the specification of the public keys of the recipients of a transfer—since, as stated above, in the Bitcoin system there is no one with whom to file a complaint and in principle we do not know the other users.

2.2 Privacy

With this, we come to the question of anonymity or privacy of Bitcoin. When installing a client application, it is not necessary to enter any personal data. Moreover, if a user chooses to use a website allowing access to the network instead of using an app, the only identification required is an email address, which could be an address created solely for this purpose using one of the many free mail services, in which it is not necessary to enter real personal data.

It is therefore, in principle, impossible to know the real identity of the person behind any public key.

There are indirect means to try and obtain clues about the identity of a determined user or, at least, the terminal from which he/she usually accesses the network, including traffic analysis techniques, IP identification, and so forth—although these mechanisms can also

[22] *The number of possible addresses is: 1.46 · 1048.*

be blocked using tools that hide or mask IP addresses, such as the TOR network.

Nor does the analysis of monetary flows to an individual guarantee any result since, as stated above, a person can create as many pairs of keys, or users of the system, as he/she wishes, creating a pair of keys for each of the transactions made in his favor or even several for each of them.

Therefore, the only means to investigate users who try to preserve their identity through the aforementioned methods is analysis of the links between transactions, which is public information. But there are other crypto-currencies that make it possible to elude investigation, such as Zcash,[23] which conceals the addresses of sender and receiver, as well as the number of transactions,[24] so that only those who have a display key will be able to see the contents of the operations.

All these difficulties have led governments and international organizations to become aware of the danger posed by virtual currencies in the fight against money laundering. For example, on July 7th (2015) the European Commission approved the proposal for Directive COM (2016) 450 final 2016/0208 (COD)[25] amending the EU Directive 2015/849 on the prevention of money laundering (EU), which already includes agencies or platforms for virtual currency exchange under the regulation for prevention of money laundering and the financing of terrorism. In such, agencies and platforms should apply controls and identify those who request the exchange between virtual and real currencies, as well as to denounce any suspicious operations. According to the text, the member states must modify their respective regulations on money laundering in this context before January 1, 2017.

2.3. Transactions

2.3.1. The Function of electronic signature processes in asymmetric cryptography systems

The process of electronic signature in this type of systems is carried out as follows:

- First, a cryptographic hash function is applied to the message to obtain its fingerprint or hash code. Therefore, hash functions return, for the element passed as input (text, images, video, etc.), a cipher summary consisting of a fixed-length alphanumeric string.

There are numerous functions or hash algorithms, such as the families MD (MD2, MD4, MD5), SHA (SHA-0, SHA-1, SHA-2, SHA-3), RIPEMD (RIPEMD-128, RIPEMD- 256, RIPEMD-320), etc. The Bitcoin system makes extensive use of this type of algorithm, not only for message signing but also for other types of tasks such as address generation, bitcoin mining, etc. One of the most used algorithms is SHA-256, belonging to the

[23] *https://z.cash/*

[24] *Dorit Ron and Adi Shamir, Quantitative Analysis of the Full Bitcoin Transaction Graph, (October 2012). http://eprint.iacr.org/2012/584.pdf*

[25] *http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf*

family SHA-2. For example, the md5 code of the first paragraph of article 1 of the Spanish Land Registration Law,[26] which says: “The Register of Property is for the registration or annotation of acts and contracts relating to the domain and other real rights over real property.” is: 7fc58fd522e15898ccf8e65ddf80697f, while its SHA-1 code is: f1a5cb06a5cae6 425a34ec11cc1314112192811dy and its SHA-256 code is: d6c59ecaa6f1cd80cb1ff 044d67134a16e23e83d3c47335af18ff72 26a72957b.

Cryptographic hash functions have several important characteristics:

• Its calculation is very simple in terms of time and the necessary calculation capacity, but, conversely, obtaining an input from its hash code is practically impossible.

• Equal entries always produce equal hash codes and different entries always produce different hash codes, so a particular hash code will unequivocally identify the incoming hash code. For example, the md5, SHA-1 and SHA-256 codes for the same text above, but without the period at the end of the sentence would be: “The Register of Property has the purpose of registering or annotating acts and contracts relating to the Domain and other real rights in immovable property a2be77b72247e97489ea6a743c203579,f96 53976b98cbd788dcd138ae84ff1e8846522 d6 and 7eb3efbbebe731b13df4a8fe67825 6e0161d7afd1ec696d0eb77a4782a20c9df.

• And, finally, it is impossible to predict any hash code from others previously captured. In the above example, we can see the great disparity that exists between the different results produced by the simple act of removing a period.

• Second, to fingerprint the message, a second cryptographic function is applied to assign it to the private key of the sending user. The result is the electronic signature of the message.

This second cryptographic function, therefore, has two entries: the fingerprint of the message and the private key of the user. It is characterized because its result can only be decrypted (and thus the fingerprint of the sent message obtained again) through the public key of the user and electronic signature of the message.

• The original message, the sender’s public key and the electronic signature of the message are then encapsulated in a single file and sent to the recipient.

• Finally, the recipient, upon receiving this encapsulated file, will use the sender’s public key to decrypt the electronic signature, included in the file, and obtain the fingerprint or hash code of the message that the sender calculated.

The recipient will also calculate the fingerprint of the original message, applying the same algorithm as the sender, and if the last fingerprint matches that

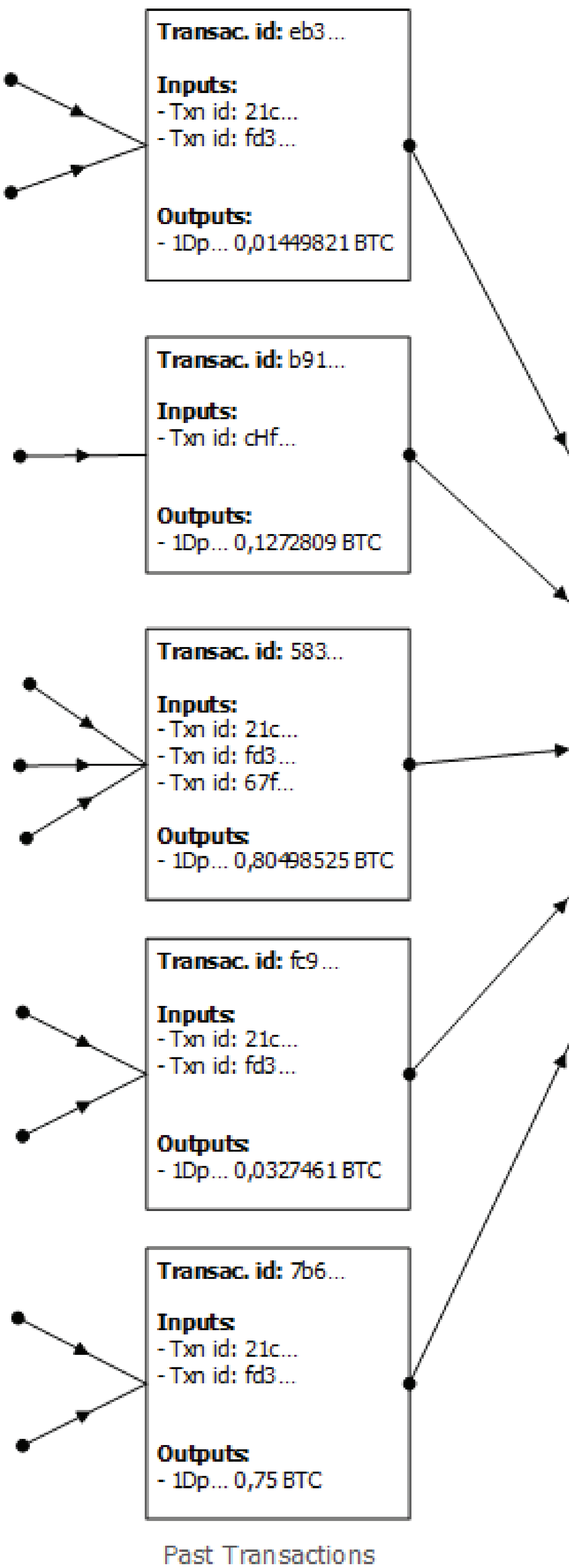
[26] *https://www.boe.es/buscar/pdf/1946/BOE-A-1946-2453-consolidado.pdf*

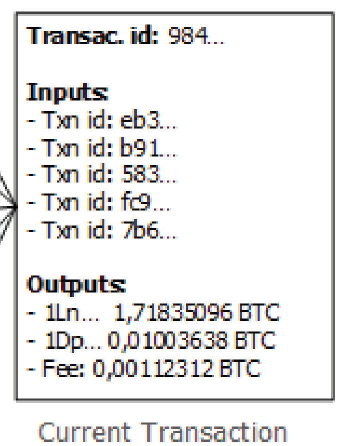
obtained when decrypting the electronic signature, it will be guaranteed that the message has not been modified and has been issued by the owner of the private key that has been used to electronically sign the message.

2.3.2. Transaction operations

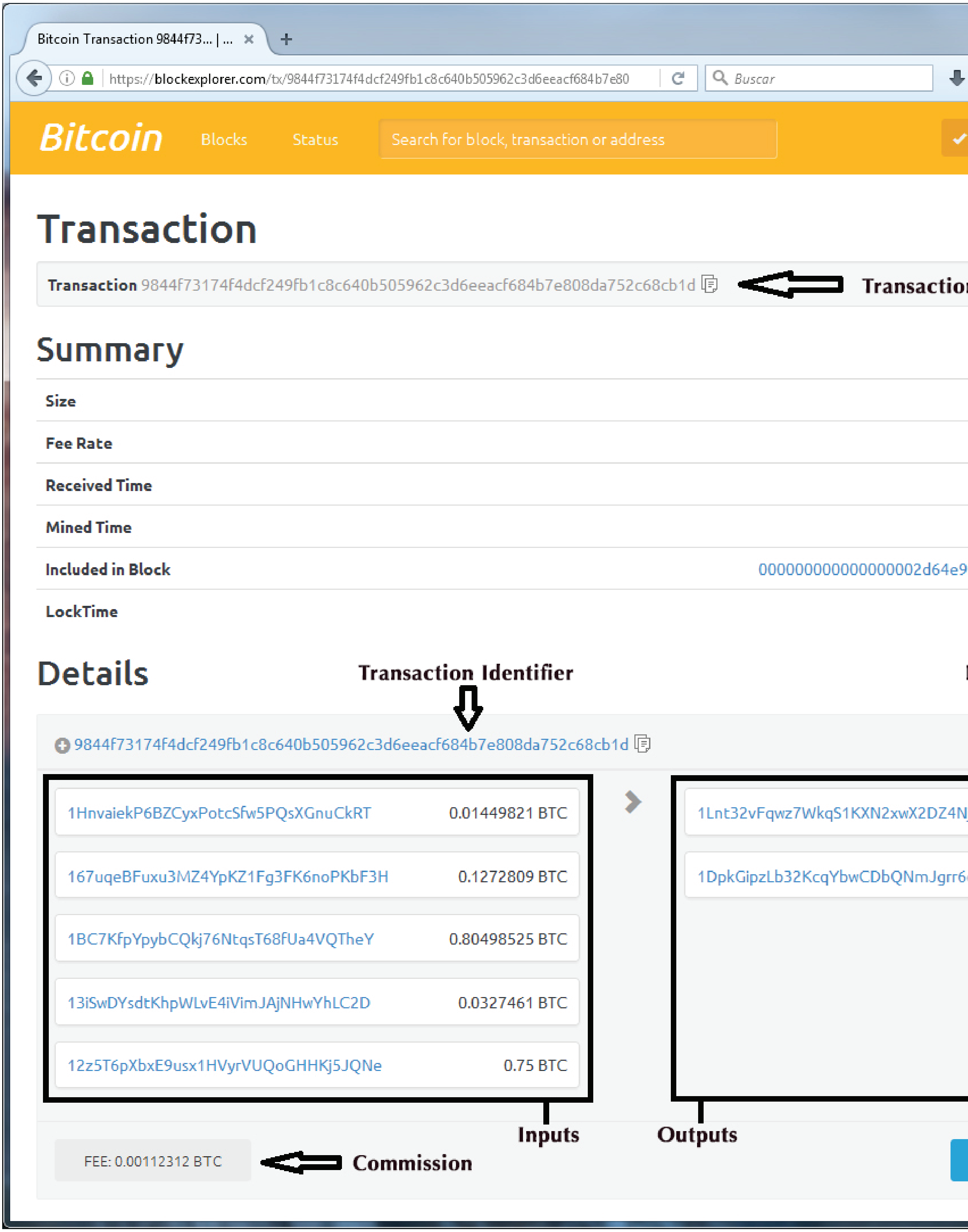
So far, we have seen how asymmetrical cryptography systems are used to ensure the authenticity and integrity of the messaging used for a transaction. However, it is necessary to look not at this aspect but also at how the virtual currencies available to a user at a given time are determined and how the transactions are stored.

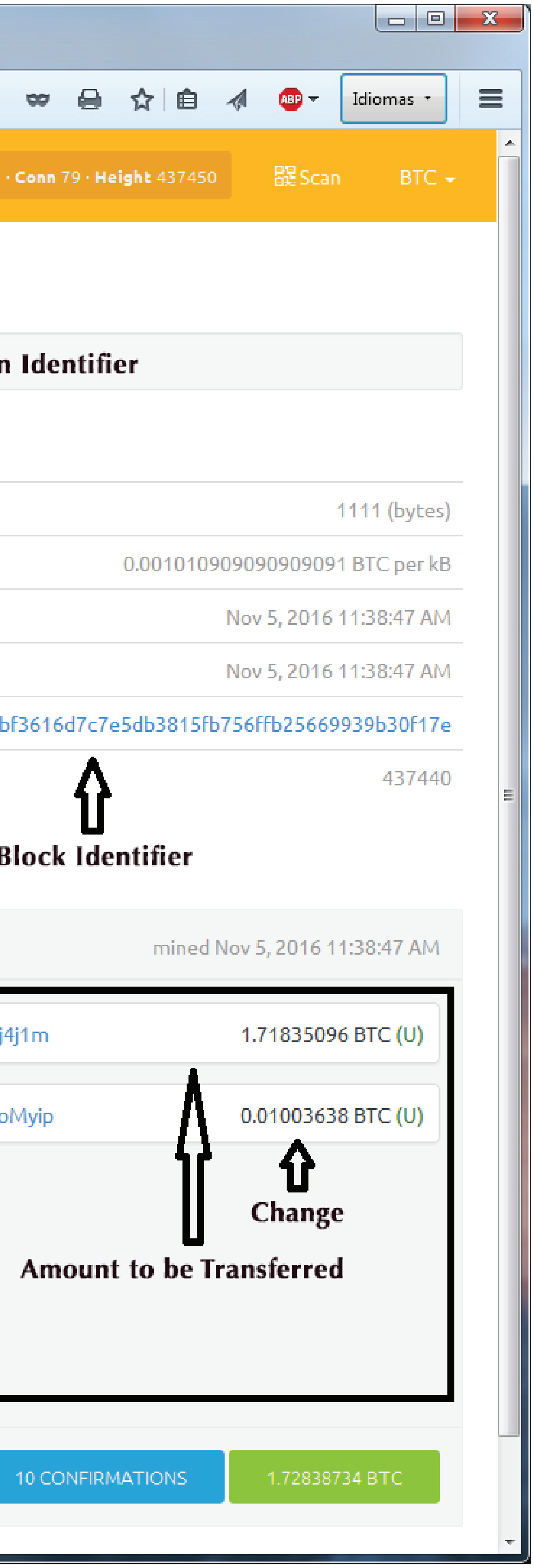
In this respect, it should be noted that the Bitcoin system does not maintain a table of balances in which the number of coins that each of the users have available at any given





graphic figure 1. transaction: 9844f7317 4f4dcf249fb1c8c640b505962c3d6eeacf68 4b7e808da752c68cb1d


Bitcoin Transaction 9844f73... | ...
https://blockexplorer.com/tx/9844f73174f4dcf249fb1c8c640b505962c3d6eeacf684b7e80
Buscar
Bitcoin
Blocks
Status
Search for block, transaction or address
Transaction
Transaction 9844f73174f4dcf249fb1c8c640b505962c3d6eeacf684b7e808da752c68cb1d
Transactio
Summary
Size
Fee Rate
Received Time
Mined Time
Included in Block
000000000000000002d64e9
LockTime
Details
Transaction Identifier
9844f73174f4dcf249fb1c8c640b505962c3d6eeacf684b7e808da752c68cb1d
1HnvaiekP6BZCyxPotcSfw5PQsXGnuCkRT 0.01449821 BTC
167uqeBFuxu3MZ4YpKZ1Fg3FK6noPKbF3H 0.1272809 BTC
1BC7KfpYpybCQkj76NtqsT68fUa4VQTheY 0.80498525 BTC
13iSwDYsdtKhpWLvE4iVimJAjNHwYhLC2D 0.0327461 BTC
12z5T6pXbxE9usx1HVyrVUQoGHHKj5JQNe 0.75 BTC
1Lnt32vFqwz7WkqS1KXN2xwX2DZ4N
1DpkGipzLb32KcqYbwCDbQNmJgrr6
Inputs
Outputs
FEE: 0.00112312 BTC
Commission



time are being updated. On the contrary, what the system does is to save the total of the transactions that are being carried out, establishing links between them that relate the current transactions with the previous ones.

Thus, in order for a user X to transfer an amount Z to another user Y, X must have in his favor, in other words pointing to his public key or identifier, a number of unused transactions totaling at least quantity Z.

Transactions that point to the user X, which will be used by the user to make the transfer to the user Y, are called inputs of this last transaction and the addresses of the user or users in whose favor the transfer is made, in this case the user Y, are called outputs.

Every transaction, therefore, must consist of a series of elements: inputs, outputs, the amount to be transferred and the transaction identifier, which is nothing more than the hash code that is calculated according to the entire set of information that makes up the transaction itself.

Figure 1 is a graphic representation of the tree of transactions for a transaction whose identifier is: 9844f73174f4dcf249fb1c8c640b5 05962c3d6eeacf684b7e808da752c68cb1dy.

It was made by the user public key: 1DpkGipzLb32KcqYbwCDbQNmJgrr6oMyip to transfer a total of 1.71835096 BTC to the user with the identifier 1Lnt32vFqwz7WkqS 1KXN2xwX2DZ4Nj4j1m.

In this figure, only the first three characters of the identifiers of the various

Figure 2. Data provided by the webpage blockexplorer.com for transaction number:9844f73174f4dcf249fb1c8c640b50596 2c3d6eeacf684b7e808da752c68cb1d

transactions and users involved are shown. Here you can see past transactions or entries in the current transaction, pointing to the user: 1DpkGipzLb32KcqYbwCDbQNmJgrr6oMyip, which were used by this to make the payment for the recipient specified above.

These entries totaled 1.72951046 BTC broken down in the following outputs: a commission of 0.00112312 BTC to the miner which mines the block in which the transaction is included (in the form presented below), the 1.71835096 BTC paid to user 1Lnt32vFqwz7WkqS1KXN2xwX2DZ4Nj4j1m, and change that is returned to the payer, user 1DpkGipzLb32KcqYbwCDbQNmJgrr6o Myip, which also generates an output in the transaction.

Figure 2 shows the output provided by the website blockexplorer.com to a query on the transaction. It has highlighted the input block, which the page shows. Transaction identifiers are not shown, but the codes of the users who made them in favor of the one that now has the funds.

Once a transaction is verified and performed by a node, it is disseminated through the rest of the network to be verified, confirmed and included in the chain of blocks by miners and stored in the local copy of each node.

Summarizing what we have seen until now, we can conclude that Bitcoin, by establishing a peer-to-peer network and the use of asymmetric cryptography, implements a system that:

- Allows for the sending of transaction messages among its users.
- Theoretically, and by using the digital signature verification mechanisms explained, can ensure that the holder of the corresponding public and private key pair is the sender of a particular transaction message.
- Manages an accounting record in which what is stored are not balances in favor of each user but the complete history of all the transactions made, as well as the relationships between them.
- In which the possibility of carrying out a new transaction depends on the validity of the previous ones. This validity is checked for each network node, for the entire transaction history, when installing the client application and downloading the existing block chain at that time and for each new transaction at the time it is performed and regarding previous transactions, or inputs, involved in the same.

Other characteristics of the transactions are as follows:

- Each bitcoin is divided into one hundred million parts that are not called centimes or pence but rather *satoshis* (in honor to the creator of the system). The minimum amount transferable is 546 *satoshis* or 0.00000546 BTC.
- Each input of a new transaction must be completely used in such a way that, if

the number of bitcoins associated with that input is greater than the amount to be transferred, that transaction will have a return output, or change. The difference shall be returned to the payer, or to another user specified by the payer.

• Each transaction can have one or more inputs and, likewise, one or more outputs. In turn, the inputs can be from one or several users, in which case they will be required to sign the transaction, and the outputs can also be addressed to the same or several recipients, which allows to reduce costs because only one fee is paid for a transaction in which several transfers are grouped.

• At present, it is not mandatory to pay a commission when making a transaction (since there are still miners that validate these type of transactions). If it is paid, however, the transaction will be confirmed more quickly. The amount of the commission depends not on the amount to be transferred, but on the number of inputs and outputs of the transaction in question.

• Once a transaction message is signed and sent, it will reach its recipient within seconds. At this point, however, it is an unconfirmed transaction, or a transaction that is not yet part of any block in the chain. It has only been integrated into a block to form part of the block chain when the transaction receives its first confirmation.

Before it has been confirmed, a transaction can be used as an entry in a new transaction, although this is not recommended. Confirmations provide security to recipients of transactions by securing their ownership over the currencies received and protect them against double-spending attacks and against the 51% attacks that will be seen later.

• Bitcoin supports a programming language: Bitcoin Scripting, which is the language used internally by the system for its operations such as sending transactions, exchanging information between nodes, etc. Bitcoin Scripting also allows code to be entered in transactions to be executed, although most of the client applications do not offer this possibility to users.

• Finally, it should be remembered that transactions cannot be reversed. If, for example, an incorrect transaction is made—a larger amount than that required is transferred or the transfer is sent to the wrong recipient, etc.—there will be no way to reverse the operation unless the user has a means to contact the recipient, if the recipient accepts the claim and if they then transfer the funds back.

2.4. The blockchain

Until now we have described the protocol that Bitcoin has established for transactions between users, but the block chains have not been mentioned. At this point the reader may be wondering if in fact these chains have some role in the system, as was stated in the

introduction to this article.

As you may recall, the creators of Bitcoin tried to establish a totally distributed system that allowed for the exchange of money and in which it was imperative to dispense with any element necessary for its operation except for one or a few controlling hands.

This implies that there is no single time signal provided to users and nodes to establish the exact moment in which a transaction is made and, on the other hand.

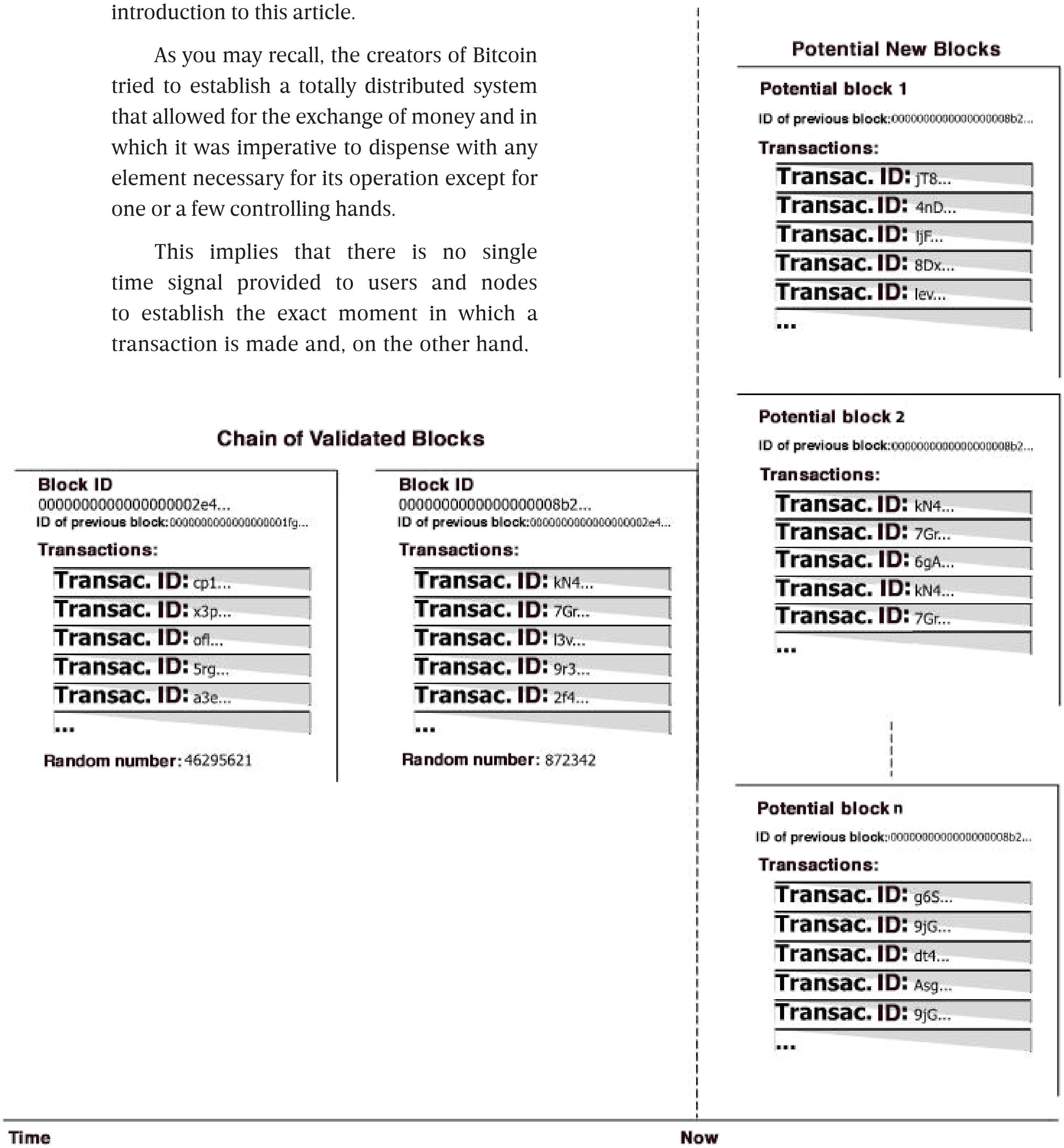


Figure 3. Representation of blockchain structure.

it is also not possible to take into account the time stamp that each user may have entered at the moment of signing and sending their transactions, since that time mark can be easily manipulated.

In this situation and given the general architecture of the system where, as we have seen, transactions are progressively communicated from node to node, it cannot be guaranteed that the order in which a network node receives transactions is actually the order in which they were made.

Because of this, the door would be opened to fraud and, especially double-spending.

Effectively, a user with bad intentions could carry out a transaction and then, before it was validated, make a new transaction from another device using the same inputs as in the previous transaction. Due to the different propagation times in the network there will be nodes that will receive the second transaction before the first transaction, and therefore will consider the latter as invalid, and vice versa, so there would be no agreement as to which operations should be considered valid.

The solution implemented in Bitcoin to solve this problem is blockchain—nothing more than a mechanism to sequence transactions.

Transactions are grouped into blocks and these are linked together, forming the block chain. A representation of the blockchain and its various components can be seen in Fig. 3.

Each block has a defined structure which must include the block identifier, the identifier or reference to the previous block,[27] the set of transactions that are grouped in the block itself (each of which will include the data described above, such as inputs, outputs, amount, transaction identifier, etc.) and a random number (called *nonce*) whose function will be explained later.

Therefore, in Bitcoin two parallel structures and with different functions are managed. First is the transaction tree whose function is to determine the ownership of the currencies and second is the blockchain whose purpose is to sequence the transactions.

Transactions included in the same block are considered to have occurred at the same time, while the reference that each block contains to the previous one allows them to be ordered in sequence.

Any node can group transactions that are not yet part of any block—that is, unconfirmed transactions—, form a new potential block and diffuse it to the rest of nodes as a proposal of the next block in the chain.

Since the different nodes of the network can make different proposals for new potential blocks, it is necessary to establish a criterion that allows for determining which of these new potential blocks should be considered the next block of the chain.

This criterion cannot be the order in which the new block proposals are received since this could result in contradictory decisions between these nodes (as has been seen in the case of transactions and because of the different speeds

[27] *All blocks, therefore, refer to the previous block except, obviously, the first block of the chain As a curiosity, the first block was mined on January 4, 2009 and its hash or identifier is: 000000000019d6689c085ae165831e934ff763ae 46a2a6c172b3f1b60a8ce26f.*

at which information is propagated between the nodes of the network).

Instead the criterion in Bitcoin is to consider valid the proposed block which has the solution to a mathematical search. This solution is the random number mentioned above in the description of block structure, and which appears in each of the validated blocks of Figure 3.

These mathematical searches are performed by the network nodes that act as miners and consist, once again, in the calculation of a hash. In this case, the hash is calculated from the data that make up each new proposed block.[28]

Specifically, the calculation is carried out on the structure of the following data set: identifier of the last block of the chain, the set of transactions that are integrated in the proposed new block on which the calculation is carried out and the random number (*nonce*).[29]

For the new block to be considered valid, and therefore the next block in the block chain, the calculated hash must be below a certain

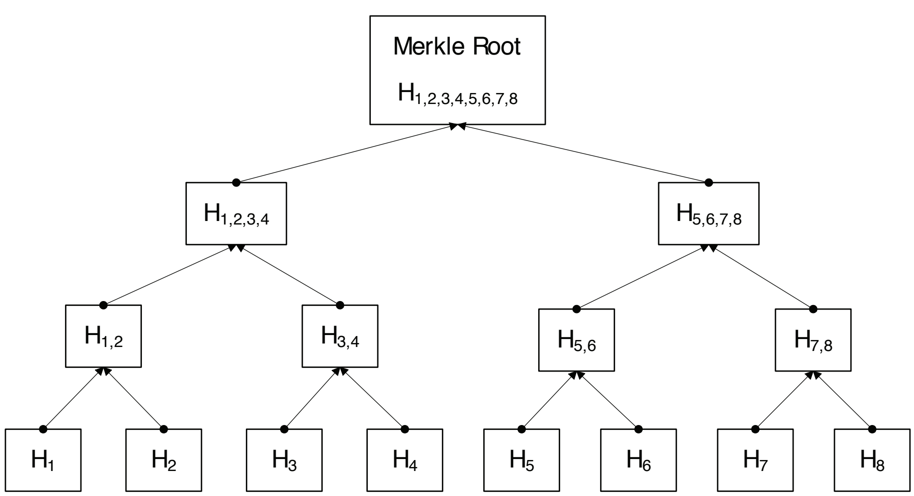
[28] *This particular hash is calculated using the Merkle tree technique:*

- Ralph Merkle. Secrecy, authentication and public key systems. A certified digital signature. Stanford University, 1979.
- Georg Becker. Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Ruhr-UniversitätBochum, 2008.

[29] *In fact, the hash of each block is the hash of the header of said block which is a field in which, among other data, the hash of the previous block, the nonce and the so-called merkleroot are stored. This merkleroot is just a new hash code that is calculated from the hashes of the transactions included in the block itself using Merkle's algorithm.*

Considering, for example, a set of 8 transactions, the following figure shows the Merkle tree for calculating the mekleroot of said set. As can be seen, transactions are grouped in pairs and a new hash is calculated (the cryptographic algorithm Bitcoin uses for this operation is double-SHA-256) from the hashes of each pair, giving rise to the Hashes H1, 2, H3, 4, H5, 6 and H7, 8. In turn these new hashes are also grouped in pairs and new ones are calculated from them, obtaining them identified as: H1,2,3,4 and H5,6,7,8 and finally, the process is repeated again to obtain the merkleroot of the set

Figure 4: Merkle Tree



*This algorithm allows a fingerprint to be obtained that summarizes all the transactions included in a block and, in turn, facilitates the verification of if a concrete transaction is included in a block, since the maximum number of operations of Hash required to perform such a check with this structure, given a set of N transactions, is reduced to 2 * log2 (N).*

value or, in other words, it must have a certain number of zeroes at the beginning (Ex: see the block identifier shown in Figure 2).

If the hash does not meet the above conditions, a new random number is used and the hash is recalculated and so on until a hash code with the required conditions is obtained.

Theoretically, on average, billions of hash calculations like the previous ones would be necessary to find the solution that validates a concrete block proposal, which would take a single computer years. However, the system itself is self-regulating, taking into account the computing power of all Bitcoin nodes acting as miners, adjusting the difficulty of the search every two weeks so that the average block validation time is kept down to around 10 minutes.

This 10-minute period is a compromise between the confirmation time and the probability of branches or bifurcations occurring in the chain (shown below). A shorter time interval for the confirmation of the blocks would make the transactions run faster, but would increase the probability of branches occurring in the block chain and vice versa.

Once the random number or nonce is produced that produces the hash with the mentioned characteristics, the block proposal is considered validated and the miner who has solved the search diffuses it through the network so that it is verified by the rest of the nodes and accepted as the next block in the list. The new block will include the calculated hash, which will be the identifier of the block itself, the hash of the previous block, the set of transactions that make up the new block, as well as the random number that solves the mathematical search.

This configuration, however, does not eliminate all potential problems as it is possible for two or more miners to simultaneously validate proposals for new, different blocks, giving rise to several possible branches in the chain.

In this type of situation, it is worth asking which of the different first blocks, of the different existing branches, will have to be considered as previous block when trying to validate a new block or, in other words, in which branch a new block must be integrated. The rule is that if all branches have the same number of blocks, each miner will continue

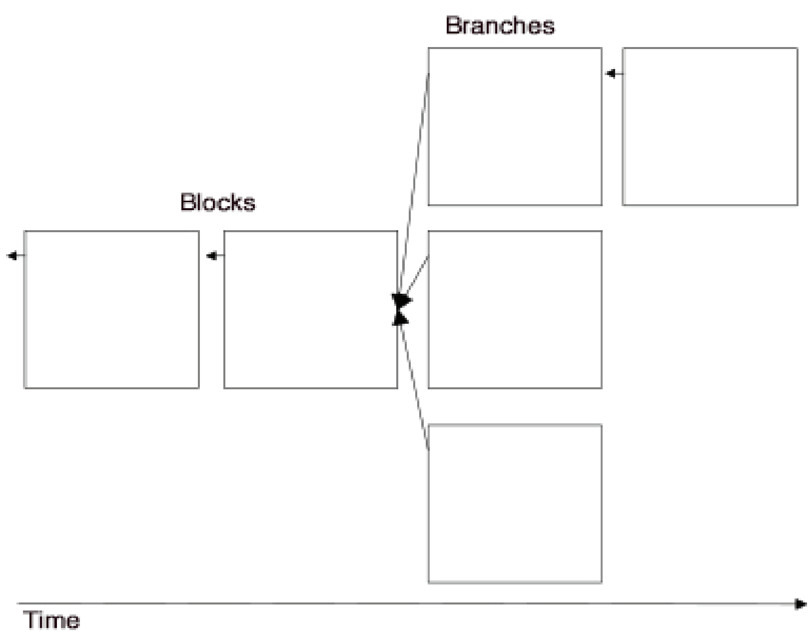


Figure 5. Branches in the blockchain

to validate blocks by considering the last of the blocks in the first of the branches he had received as the previous one. However, the moment a branch is longer than the others the miner will automatically begin to mine on this, which will also cause the rest of the branches to be removed and all transactions that were included in the blocks that were part of these shorter branches and therefore considered as confirmed transactions, will again become part of the unconfirmed set of transactions and will have to be included in a later block which, in turn, must be mined in order to be integrated again in the chain of blocks.

Unfortunately, this last circumstance opens the possibility that a malicious user can carry out double-spending (which was precisely what was to be avoided through the chain of blocks) through 51% attacks.

Let's imagine that user X performs a transaction in favor of user Y. User Y then waits for that transaction to be confirmed to provide the service or to send the product purchased by X. Meanwhile, X mines his own branch of blocks in which he/she will include a new transaction from the same entry used to make the payment in favor of Y, but to use it in favor of a different user.

When Y performs the service contracted by X, Y sends the mined branch to the network, which, if it is longer than the branch that contained the original transaction, will replace it and, therefore, unconfirm the original transaction in favor of Y.

When this happens, you will have lost your money because when you try to confirm/reinstate the transaction in your favor, the system will detect that the input used by X to pay has already been spent on another operation and will be invalidated.

Since X cannot modify a block in the chain by substituting one transaction for another (this would be detected immediately by the verification of hashes) the only way is to compete in a mathematical race with all other nodes in the network to build a longer branch than the one constructed by them. In order to do so, X should control more than 50% of the total computing power of all the nodes/miners that make up the network, hence the name "51% attacks".

It is generally considered that the probability of a successful 51% attack is negligible given the large number of miners composing the Bitcoin network. In any case, it is recommended to wait for a transaction to be confirmed by at least six nodes before providing the product or service.

In fact, it is possible to show[30] that:

- It is not necessary to control more than half the calculation power of the Bitcoin network, but rather, it is possible to successfully carry out the attacks described above whatever the computing power of an attacker.
- The greater the number of confirmations a transaction receives, the less likely it is that a double-spending attack is successful. The speed in decreasing this

[30] *Meni Rosenfeld, Analysis of hashrate-based double-spending, (most recent version, February 2014). https://arxiv.org/pdf/1402.2009v1.*

probability will depend on the computing power available to the attacker.

However, no number of confirmations will decrease the probability of a successful attack to zero. Rather, if the attacker has more computing power than the rest of the network (that is, more than 50%), no number of confirmations will reduce the success rate below 100%. In fact, a malicious user of the latter type will not only be able to carry out a double-spending attack on any transaction, but may also force any block not mined by it to be rejected.

- The recommendation to wait for 6 confirmations mentioned above is based on the assumption that an attacker is unlikely to be able to control more than 10%[31] of the net computing capacity, and that a 0.1 probability of a successful attack is acceptable. However, although the criterion of the six confirmations can discourage the occasional attacker, it is not an insurmountable obstacle for an attacker who actually has more than 10% of the computing power.

2.5. The problem of block size

When Bitcoin protocol was designed, a relatively low block size limit of 1 MB was set in order to make denial-of-service attacks more difficult. The result is that the maximum transaction processing capacity per unit of time is reduced to approximately 7 transactions per second, since a block is mined every 10 minutes and the size of each transaction is about 250 bytes, since there is a limit of around 4,000 transactions[32] that can be grouped in each block.

In comparison, ordinary financial operators have much higher processing speeds (VISA, for example, can process thousands of transactions per second), making it difficult for Bitcoin, in its current configuration, to be adopted as a global payment system given the scalability problems that could arise in the future.

This has caused the size of the blocks to become one of the main concerns within the Bitcoin community and has also led to division, confrontation and abandonment among core developers, miners and the companies that lend Bitcoin services as to whether the limit on block size is a problem and, if so, how it can be solved.

Arguments have been made for and against increasing block size:

In favor:

- The aforementioned need to increase the processing speed of transactions in order to compete with other established payment systems.
- If processing speed is not increased, the fees that users have to pay miners to validate and mine their transactions as soon as possible will increase, discouraging use of the system.
- It would create space for the implementation of extensions of the Bitcoin protocol like metacoins,

[31] *In fact, this happens more frequently than might at first be believed. Thus, for example, during the first months of 2014 the mining company Ghash.IO (https://ghash.io) was very close to reaching 50%; Several groups of miners (AntPool, F2Pool and BitFury, etc.) each more than 10% of the total computing capacity, and there have also been groups such as BTC Guild (now Extinguished), which have been able to solve branches of up to 6 consecutive blocks.*

[32] *at https://blockchain.info/es/charts/n-transactions-per-block?timespan=all you can see the average number of transactions per block*

metachains or blockchainapps (Colored Coins, Mastercoin, Counterparty, etc.). These extensions are characterized by sharing Bitcoin's block chain, but add new layers to the protocol that allow you to include additional data in transactions.

Against:

- Higher fees, or simply the need to pay some kind of fee, will eliminate spam transactions and financially incentivize miners not to abandon the system, especially since the reward they receive for mining blocks will be reduced progressively, as explained in the following section.
- It will increase the likelihood of branches occurring in the chain and, therefore, a greater probability of double-spending situations, since the larger blocks will imply slower propagation speed and also require greater node processing capacity.
- Lower propagation speed and the need for greater processing capacity will cause the Bitcoin network to be more centralized, as the number of miners will fall due to increased cost and, therefore, the system's security will decrease.
- Increasing the size of the blocks would, in any case, be a transitory measure since no specific size will ensure that there are no future scalability problems.
- A fork in the block chain (hardfork) would be necessary since a new, completely incompatible version of the system would be implemented.

This fork would be a planned bifurcation requiring the abandonment of the old chain of blocks, therein the unanimous acceptance of the new version by all the actors in the system, and its migration to the new chain.

But given the number and the strong opposing interests of different users, such unanimity is considered virtually impossible. The realization of this hardfork would most likely result in catastrophic consequences for bitcoin reputation and price.

In any case, the truth is that several proposals have been published for increasing block size (Bitcoin Improvement Proposal or BIP),[34] some of the best known being: BitcoinClassic, BitcoinUnlimited, Bitcoin XT. The latter, for example, was published in August 2015 by Gavin Andresen and Mike Hearn (both had previously been Bitcoin's main developers) and consists of a variant of the BIP 101 proposal, in other words, to increase block size on January 11, 2016 from 1 Mb to 8 Mb, doubling it again every two years, until it reaches 8192 MB. Protocol improvements would be added to make it difficult to double expense, DDoS attacks, improve the node identification, etc. The proponents also believe that Bitcoin XT should be compulsorily adopted by all nodes, once it has been accepted and installed by 75% of the mining nodes.

However, acceptance among the bitcoin community was not as strong as the authors had expected (you can check the

number of nodes using Bitcoin XT, and also BitcoinCore or traditional, BitcoinClassic and BitcoinUnlimited, compared to the whole network at: http://xtnodes.com/#all_nodes). Bitcoin XT is installed in only slightly more than 1% of all nodes, and yet what has occurred is a strong internal struggle, a kind of civil war within the bitcoin community, starting with its five main developers: Andresen and Garzik are in favor of the aforementioned hard fork, but the other three have totally rejected it.

Likewise, there have been conflicts between miners, together with computer attacks to collapse the nodes that implemented Bitcoin XT. Companies that provide services around Bitcoin have been involved in the block size problem, as well as in the conflicts described. Some entities such as Blockstream have been accused of opposing the increase in block size head-on exclusively for business profit reasons, as these companies could therefore impose the use of their own technical solutions to the problems of maintaining the current size[35] (In the case of Blockstream, its solution is called Lightning Network),[36] charging users the corresponding fees for its use.

All this finally provoked the retirement of Mike Hearn in January of 2016 through a bitter article[37] in which he announced the sale of all his bitcoins. He stated that he considered Bitcoin a failed experiment describing its numerous problems, among which he mentioned the already mentioned

[34] *Some of the main proposals in this area have been the following:*

- *BIP 100: Published by one of the main developers of Bitcoin: Jeff Garzik in June 2015. It consists of the size of the blocks is not fixed, but, every 12000 blocks (about three months), the size of the block Will decide by vote among the miners, with a maximum limit of 32 MB. A variant of this proposal is known as BitcoinUnlimited.*
- *BIP 101: Published by GavinAndresen, also in June 2015, and proposes the expansion of the block size to 8 MB, increasing successively every two years, reaching 8192 MB, and as the capacity of the processors increases - according to Moore's Law, the storage capacity and bandwidth of communications networks. Later, GavinAndresen along with Mike Hearn, would create a variant of this proposal, called Bitcoin XT.*
- *BPI 102: by Jeff Garzik, it was an emergency proposal, as a way to save time in case there was no consensus. However, since it was only an emergency proposal, it did not contain a medium- and long-term strategy on block size. It consisted of expanding the block size to 2 MB as of November 11, 2015.*
- *BIP 103: proposed by PieterWullie (Blockstream) in August 2015 and consists of increasing the maximum block size by 17.7% each year, from January 2017, to 2 GB by 2063.*
- *BIP 109: Another proposal of GavinAndresen that also consists in increasing the block size to 2 MB and that, along with other additional measures, would later crystallize in the proposal known as BitcoinClassic.*
- *BIP 141: Also known as SegregatedWitnes or SegWit and PieterWuille proposal. Basically it consists of transferring the signature data of the transactions to a parallel data structure, so that the size occupied by each transaction in the blocks is reduced and could be included more in each one of them.*
- *Proposed Adam Back (Blockstream) blocks in which 1 MB blocks would be maintained, but miners wishing to use larger sizes (10 MB) could do so. This proposal would involve the creation of two different block strings on the same Bitcoin protocol.*
- *Proposal by Sergio Lerner, which consists of maintaining the maximum limit of 1 MB, but accelerate the mining of blocks in such a way that would move from the current 10 minutes per block to 5 minutes per block.*

[35] *https://www.reddit.com/r/btc/comments/42nx74/unmasking_the_blockstream_business_plan; http://xtnodes.com/announcement.php; https://bitco.in/forum/threads/gold-collapsing-bitcoin-up.16/page-59#post-2245; etc.*

[36] *https://blockstream.com/technology/#sidechains*

[37] *https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.ewfepr21j*

lack of capacity to process increasing transactions in the future which will result in the collapse and abandonment of the system, the monopolization of virtually all mining capacity by a few groups who oppose any modification that may affect their current status, also implying the loss of control of Bitcoin by users, which was one of the initial objectives. Hearn also mentions the lack of clarity regarding the amount of fees payable for execution of transactions and their foreseeable rapid growth, the lack of democracy in the Bitcoin community, among other issues.

In any case, the problem of block size and the consequential reduced processing capacity of transactions per unit of time remains a problem waiting for a solution.

2.6. Miners

As we have seen, one of the main functions of network nodes acting as miners is the construction of the blockchain. Miners are also the means for the generation and distribution of new coins in the system since every time a valid block is built, the miner receives a reward in the form of newly created bitcoins (although he/she must wait for another 99 blocks to be mined before receiving the reward).

Every time 210,000 blocks are mined, which, at minimum speed of 10 minutes per block, occurs approximately every four years, the reward is halved. 2016 was one of the years in which this reduction took place. While up until last July 9 the amount paid miners for each mine block was 25 bitcoins, the amount was then reduced to 12.5 bitcoins. With this progression, the total number of bitcoins to be created will be approximately 21 million.[38]

Another source of income for miners, as mentioned earlier, is the collection of fees that users pay to speed up the confirmation of their transactions. Payment of these fees is not mandatory if you do not want priority to confirm a transaction, but in the future, when the reward system ceases or when they cease to be profitable, fees will be the only source of revenues for miners. Because of this, transactions will cease to be free and the fees are expected to grow considerably.

In the early days of the system, miners had a mainly domestic character, using their own personal computers to mine bitcoins. But as the value of the currency rose, miners began to professionalize and partner to distribute profits.

In parallel, custom hardware and processors for mining bitcoins began to be designed and built (ASIC's or application-specific integrated circuits),[39] which have been doubling their processing capacity about every 6 months. Today one of these machines has capacity of tens of tera-hashes per second.

[38] Therefore, bitcoin is a coin with a progressive, controlled and limited supply (until reaching the amount of 21 million coins). During the first years of Bitcoin's life, from 2009 to 2012, the reward for the mines of each block was 50 bitcoins. On November 28, 2012, block number 210,000 was mined and the reward became 25 bitcoins; Subsequently, on July 9th, block number 420,000 was mined and, once again, the reward per mine block was reduced by half, that is, to an amount of 12.5 bitcoins and approximately in another 4 years, In 2020, will be reduced to 6.25 bitcoins. With this progression it is estimated that in the year 2140 the last bitcoin will be generated.
at http: //www.bitcoinblockhalf.com you can check the countdown until the next reduction in the reward of the miners

[39] https://www.bitcoinmining.com/bitcoin-mining-hardware.

There is also the possibility of contracting mining capacity in the cloud from companies that provide this type of service.[40]

All this has led to the emergence of "farms" housing thousands of specialized machines dedicated exclusively to the mining of bitcoins, which have practically eliminated the possibility of domestic or occasional miners being able to mine a block. On the other hand, mining is an activity with high energy consumption: one of the main costs (about 90%) faced by miners is the cost of electricity to function. This has led most mining farms to set up in countries with low electricity costs, either because they have no strict environmental standards and make intensive use of energy sources such as coal for electricity generation (as is the case in China, Georgia, Mongolia and Malaysia) or have a large amount of renewable and cheap energy, such as Iceland.

2.7. Blockchains and Title Registration

In title registration systems, cases that are annullable, invalid, incomplete, irregular or challengeable may be submitted for registration, but registrars will reject them, thus preventing such acts from gaining the disclosure of registration. This happens in the independent check for legality that registrars conduct and for which they are accountable.

The exhaustive legality check upon which registrars base their decision as to whether to register or reject a legal transaction is an indispensable condition if registration is to guarantee the *in rem* third-party protection effects that are characteristic of title registration. If a registrar registers a title, that title is then recognized by the state, and the party named as the holder of the right at issue in the title is considered the holder erga omnes, with the breadth and restrictions stated in the registration entry.

Note that the model I have just described is exclusively institutional, but could be supported by a technological infrastructure. Such an infrastructure would in all cases be merely instrumental. The question is whether an equal or higher level of legal certainty can be attained with an exclusively technological/computerized model based on blockchain technology.

There are two versions of blockchain-based models that could be applied to registration. First is what we might call the "hard" version, which would basically consist of a public, self-managed blockchain working like the Bitcoin blockchain. Instead of coins, the system would store smart contracts sent by the parties who signed them. Rights and charges on real property would be created and transferred through these smart contracts. The blockchain would be replicated in the nodes of a free-access peer-to-peer network having the same kinds of nodes as in Bitcoin, where miners would validate transactions

[40] *for example: Eobot: https://www.eobot.com; GenesisMining: https://www.genesis-mining.com; Ghash.IO: https://ghash.io; HashFlare: https://hashflare.io; HashNest: https://www.hashnest.com; MineOnCloud: https://mineoncloud.com; MinerGate: https://en.minergate.com; Minex: https://minex.io; NiceHash: https://www.nicehash.com; etc.*

by performing mathematical searches resembling those we described before and would be recompensed with some sort of virtual money.

The second is a "soft" version, which would consist of a private blockchain used only as a mechanism to provide technical security for registration entries while maintaining the institutional title registration model described above.

As we will see, systems based on the hard version not only fail to increase the preventive legal certainty title registration provides; they drastically reduce it. Meanwhile, systems based on the soft version are ultimately no more than one of many technical alternatives for storing and securing information.

There are certain characteristics of the blockchain operating protocol (at least in the hard version) that are actually incompatible with the objectives that registration systems pursue and the rule of legal certainty that registration systems serve.

First, there is the issue of privacy. As we have seen, users in a blockchain system are identified only by their public key. No other data enabling a user's real identity are stored or even exist. This does not correspond with the way registration systems operate. Registration systems are nothing if not a mechanism of transparency, of disclosure. Their goals include disclosing the ownership of property, disclosing the rights in and charges against property and eliminating hidden charges. Above all, the object of registration is to give trade operators confidence and thus facilitate territorial credit and, in short, contribute to economic security.

Furthermore, identifying the holders of registered rights facilitates the transfer of those rights. In an unidentified-holder scenario, right transfers are frustrated if the holder loses the private key or dies without giving his or her heirs access to it.

In addition, registration is also a powerful mechanism for helping satisfy a range of general interests, such as fighting crime (e.g., corruption, money laundering), which also requires the real identity of registered holders to be known.

Another incompatible point is personal data protection. It is true that registration systems are systems of disclosure and transparency, but this doesn't mean all the information a registration entry contains ought to be open to public access. Personal data protection rules and personal privacy rules need to be respected as well. On the other hand, as explained before, all the information stored in blockchains can be freely accessed by anybody, regardless of whether the person doing the accessing is a party to the transaction involved. This is an especially sensitive subject in Europe, and it has accordingly been copiously addressed in

a great deal of EC legislation.[41] The subject is one directly related to fundamental rights and is therefore reflected in many constitutions. Some constitutional courts have established case law viewing the right to personal data protection as one that is independent of but intimately related to the right to privacy and closely linked in some cases to freedom of ideology. There are countries where registrars are required to protect the personal data included in registration records.

For all these reasons, free and direct access to the contents of registration entries cannot be allowed. Anyone wishing to consult registration details must be forced to show proof of a legitimate interest first.

Another point of friction between blockchain operation and title registration operation is how priority is assigned to the rights entered in each system. In blockchains, the order of transactions does not depend on the instant when transactions are performed and sent; it depends on a totally random act that is completely unrelated with the parties to the transaction: the solving of the mathematical searches miners perform in block mining and transaction validation. A transaction that is initially confirmed and included in a mined block could even be "deconfirmed" if it lies in a block on a branch that turns out to be shorter than other branches at some given point in the chain.

In many title registration systems, the time when documents are submitted for registration (whether in person or online) is what determines the priority of the rights those documents refer to, and a timestamp is applied accordingly. This way, the holder of a right can know the status of the property's record at the time of submission and know exactly what rank his or her mortgage will hold in comparison to everyone else's.

Let's imagine the blockchain protocol is applied to registration. If various submissions are made successively concerning the same property, the submitters have no way of knowing what rank or priority their rights are eventually going to hold after registration. The right created and submitted last of all could even be entered before the right submitted first; due entirely to random factors (block mining) or monetary factors (if the last submitter paid a higher commission than the others), the block holding the last transaction might well be mined first. And things could become even uglier if an initially registered right is later "deregistered" due to having been placed in a short branch.

Obviously, this would create legal uncertainty instead of legal certainty. And obviously, it would hamper trade, because trade operators would never be able to be entirely certain that, when they sign registrable contracts, the status of registrable rights they

[41] See, for example: the Charter of Fundamental Rights of the European Union of 7 December 2000; the Treaty of Lisbon, 13 December 2007; Regulation (EC) No 45/2001 of the Parliament and of the Council of 18 December 2000; Regulation (EC) No 2725/2000 of the Council of 11 December 2000; Regulation (EU) No 611/2013 of the Commission of 24 June 2013; Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016; Directive 2002/58/EC of the Parliament and of the Council of 12 July 2002; Directive 2006/24/EC of the Parliament and of the Council of 15 March 2006; Directive (EU) 2016/680 of the Parliament and of the Council of 27 April 2016.

have looked up in the registration records at the time of signing is the definitive status. Nor would they be able to be sure of the priority their right would have in relation to other rights submitted for registration at roughly the same time. For example, it would be possible for a right B, created and submitted after right A, to be registered with priority over right A due to the random operation of the blockchain and thus cancel out right A.

Even so, the main reason why systems implementing the hard version of blockchains cannot have the same effects as a title registration system is that blockchain systems conduct no check of legality or scrutiny of form whatsoever.

Real estate deals are very important for a country's markets, credit and economy. For that reason, real estate contracts are enveloped in special precautions and solemnities, especially in countries that have title registration systems, which, as we explained before, try to avert all future litigation with respect to registered rights as a means of creating certainty and confidence in business dealings.

Its really is not enough for the parties to sign a contract. There has to be some verification that nothing can render the contract void or ineffective. For example, someone has to ascertain not only that consent was truly given, that the persons who consented to the contract are who they say they are, that they gave their consent freely, that they were not incapacitated or limited in their powers of disposal, that the parties were of sound mind and, if one of the parties acted through a representative, that the representative really held the power to represent the party and was given the right faculties to carry out the legal act at issue in the contract, and so on. Moreover, someone has to check that the various component circumstances of the deal are legal and do not affect pre-existing third-party rights. None of these issues are dealt with by blockchains.

You might say that these issues could be at least partially addressed by standardizing the kinds of contracts that can be registered. Then, only rights contained in pre-established contract forms signed by the parties would be admissible or registrable. Such a course of action would, however, clash with freedom of enterprise and freedom of contract, both of which are traits of the modern market economy.

It would therefore seem illogical to purposefully choose a technical solution that involves or requires reducing citizens' legally acknowledged freedoms, especially since there are other options that enable those freedoms to be upheld. Picking the hard blockchain would make it seem like the technology is the truly essential item in the process, rather than a mere accessory or instrumental component. And that would lead ultimately to a scenario where the only contractual relationships people could have would be the contractual

relationships that the technology can handle, in the mode and form mandated by the technology—an unacceptable situation.

We must not lose sight of the fact that registration is not just for contracts. Judicial and administrative authorities issue registrable decisions, decisions that can adapt registered rights, cancel them, order new property or rights registered, set restrictions on transfers, and so on. Limiting courts' independence to determine the contents of their own decisions by establishing pre-set forms is not feasible.

Account must also be taken of the fact that registrars do not only reach an independent judgment on whether contracts are lawful and respect third parties' rights (acting like an ombudsman for everyone not present); registrars also apply consumer protection law in the defense of the parties to each contract.

Consider this: In the hard version of blockchain real estate contracts, in which completed contracts are sent to the chain for "registration", eventually almost all contracts would wind up being adhesion contracts. Without a registrar's legality check, the parties uninvolved in the drafting of the contract stand at a permanent disadvantage.

Blockchain users could be hurt even worse by the fact that the system would not provide them with any of the personal, direct legal advice registrars furnish. Users would have to go to outside legal consultants for advice, at additional cost.

It could be argued that some of the drawbacks of the hard system could be avoided by choosing the soft version of the blockchain system, that is, by establishing a private blockchain system in which documents must undergo a registrar's scrutiny before the information is entered in the chain. This could be feasible, but also means that some of the main traits making the blockchain what it is would be lost, such as the elimination of privacy, mathematical searches for arranging transactions in order, and so on. The soft system would increasingly resemble other technological options that furnish the same guarantees, such as the Spanish model which applies electronic signature technology to documents and entries and uses electronic timestamps and data replication clusters.

Blockchain Technology: the Last Mile for Electronic Land Registry Systems

Adriana Jacoto Unger, Joao Marcos M. Barguil and Flavio S. Correa da Silva
Universidade de São Paulo, São Paulo (Brazil)

Introduction

Since the advent of blockchain—the technology underlying crypto-currencies allowing for permanent registry in a distributed digital ledger—property and land registry has been identified as one of the most promising fields to be transformed, replacing traditional trust intermediaries with blockchain peer-to-peer transactions. Many initiatives the world over (in countries such as Sweden, Honduras and Ghana) have begun the process of preparing their property registry systems for migration to blockchain. Such changes envision modernization: automation, data interoperability, improved services, cost savings and enhancement of security and transparency in land property exchange activities.

Despite the technology hype surrounding blockchain, migrating paper-based Land Registry systems—oftentimes a hundred years old—that rely on well-established trust authorities to a fully digital system based on blockchain is a challenge that should not be underestimated. Values intrinsic to the old system such as the longevity and integrity of

registries, authenticity of identity and registry data structure standards may be lost in a new system if not well integrated in the architecture of electronic Land Registry systems. Conversely, long-held registry practices well suited for a paper-based registry system may not be well suited when reproduced in a digital system, resulting in technology that increases, rather than decreases, inefficiency.

Blockchain and Land Registry

In the first years of the Internet and the first e-commerce endeavors, one difference between bits and atoms became clear: unlike atoms, bits can be copied indefinitely while maintaining content and integrity. On one hand, this allowed for the massive dissemination of information and democratized communication on a global scale, since bits can be shared and exchanged freely in the web. On the other hand, commercializing digital assets over the Internet (such as music, movies or news) has always been a tough challenge for the same reason. One of the biggest innovations blockchain technology brings to the forefront is the possibility of having a unique digital asset (one unit of cryptocurrency, for example) that can be exchanged over the Internet in a fraud-proof system.

The appearance of applications based on blockchains at the end of the last decade sparked new interest in the development of fully decentralized, autonomous systems. The concept of blockchain was first introduced by Bitcoin,[1] a peer-to-peer electronic cash system. Its security is based on cryptographic primitives, and for this reason it is known as the first cryptocurrency to have widespread presence. More recently, blockchain-based systems have been proposed as means to implement other kinds of decentralized applications[2] in which nodes are capable of trusting the information that flows through the system, even though they are not expected to trust each other (nor is there a central source of truth).

Blockchain is grounded on the notion of a distributed ledger, which acts like a database available to all peers. Each peer has their own copy of the ledger, containing information about the history of transactions in the system. It is constantly audited by groups of agents selected according to different policies, depending on the application domain. The result of each auditing round is stored in a block and broadcast to the network. Blocks are sequentially appended to the ledger, forming a cryptographically linked chain. Attempts to tamper with blocks or to alter their order can be easily detected. The whole community of agents may accept or reject the reliability of any block according to a predefined set of rules. If an agent receives several valid additions to their local copy of the ledger, they

[1] *Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.*

[2] *E. C. Ferrer. The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695, 2016; A. Lazarovich. Invisible Ink: blockchain for data privacy. PhD thesis, Massachusetts Institute of Technology, 2015; Y. Lewenberg, Y. Sompolinsky, and A. Zohar. Inclusive block chain protocols. In International Conference on Financial Cryptography and Data Security, pages 528–547. Springer, 2015; S. D. Norberhuis. MultiChain: A cybercurrency for cooperation. PhD thesis, TU Delft, Delft University of Technology, 2015; K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles. A blockchain-based approach to health information exchange networks.*

always choose the longest chain of valid blocks (or the earliest one, if they have the same length), ignoring other conflicting and less relevant chains. This ensures that consensus is eventually reached, even in scenarios where propagation is slow due to high network latency. Similarly, ill-intentioned agents may try to insert malicious entries in the ledger, but the community will simply reject their blocks and ignore their chain, efectively forcing them to abide by the rules.

Ethereum[3] is a blockchain-based platform for fully decentralized applications. It is based on the notion of smart contracts, which are procedures that determine sequences of actions in order for peers to interact with one other. It is a step further on the scale of autonomous systems: while in Bitcoin it is only possible to define transactions such as "Transfer X tokens to account Y", in this more elaborate scenario it is possible to define interactions like "Transfer X tokens to account Y if, and only if, they can prove that they have finished the job they have been hired for." The system efectively works as real-world contracts do, but in a completely autonomous fashion. Based on this platform, it is possible to define reliable decentralized systems in which transactions can only happen if they fulfill the rules defined in each smart contract (if one is defined).

Because of its flexibility and support for the definition of arbitrary smart contracts, the Ethereum platform could be considered a viable alternative for the implementation of an electronic Land Registry system. And the fact that it is open-source and supported by various entities including big technology and financial corporations[4] also weighs positively in its favor.

First things first

Architecting an electronic Land Registry system involves the challenging but imperative task of digitalizing land registries. All aspects of security requirements (privacy, authenticity and integrity) must be considered in order to guarantee that the purpose of the Land Registry business process will be maintained in the new system.

A digital standard for data structure to be recorded on the blockchain must also be defined, considering not only the legacy of registry data currently available, but also expected new functionalities such as data interoperability and georeference.

In Brazil, the SREI project[5] was developed to analyze the current paper-based Land Registry system and define the architecture of a new Electronic Land Registry System. The proposed architecture maintained the current registry system for property rights, allowing registry offices to act in the legal role of anticipating and preventing judicial disputes involving properties. In addition, it offered a complete redesign of property legal status updates, allowing for more efficient operations at Registry offices. Moreover, data exchange requirements meant the architecture had to

[3] *G. Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014.*

[4] *Robert Hackett. Big business giants from Microsoft to J.P. Morgan are getting behind Ethereum.*

[5] *IRIB. SREI Sistema de Registro de Imóveis Eletrônico. http://folivm.wordpress.com/, 2012*

consider a molecularized network of registry offices, as opposed to previously atomized and isolated registry offices. The new organization and data standardization led to the creation of a regulator (National Registry Operator), responsible for coordinating all efforts to keep the new Electronic Property Registry System working and evolving.

The last mile

The SREI project defined a security mechanism for electronic Registry as a chain of data blocks secured by a series of cryptographic signatures, yet still centralized. The advent of blockchain technology offers enhanced possibilities of implementation of such mechanisms in the Electronic Property Registry System, without discarding any of the valuable results of the new architecture to the overall improvement of national property registry system.

Once the foundation of the Electronic Land Registry System has been defined, it will be easier to focus on the technological challenges of blockchain implementation itself, the core of the electronic property registry. Any blockchain initiative should be preceded by the careful establishment of a benchmark for technology platform selection, considering specific features and purpose of the property registry system. Despite the fact that Ethrereum smart contracts may seem very suitable to implement Land Registry business rules, numerous other distributed ledger-based technologies are currently being developed, considering the wide range of applications addressed by blockchain technology. Furthermore, more recent advances in private blockchain development and their ability to interact with public blockchains may offer an interesting solution to address the problem of maintaining privacy of property registries while allowing for registry publication.

Conclusion

New technologies often pose a threat to established business and, at the same time, bring opportunities for new business and the transformation of business relationships. Blockchain for Land Registry is no different in this aspect, as it appears to threaten to replace the role of Registrars with new technology. But a close look at recent blockchain business cases, mostly in the financial industry, shows that mainstream companies are the ones most investing in blockchain development, with the intent of transforming rather than replacing trust chain, as interested players are involved in the development of new technology.

What does Blockchain Registry Mean for the Owner?

Teófilo Hurtado Navarro, Land Registrar
Felanitx, Palma de Mallorca (Spain)

Abstract This article is about the impact of blockchain on registered property rights. The author points out the need to distinguish between different land registry systems, asserting that blockchain is better suited to those systems operating only as archives than to advanced title registry systems. Blockchain benefits notary activities but not title registry systems where, rather than offering added value to existing technologies, it brings new complications. In land registries, judicial decisions and administrative resolutions are also registered. Blockchain fails to provide more security for registered rights.

There has been much talk in recent times about blockchain and its possible use in different fields, including real estate transactions. Despite the large number of articles and conferences devoted to the subject, most have been limited to explaining, both more and less precisely, the technical aspects for the uninitiated, or the economic advantages that their implementation could present.

However, it should be noted that, whenever blockchain-based land registry is explained, little attention is paid to the legal implications that such a system would have on the ownership rights over immovable property. This may be because companies dedicated to blockchain development are made up of computer scientists and not legal professionals, or perhaps because the legal systems they use as references

are so limited that they need nothing more than blockchain to overcome their shortcomings.

We shall see, however, that blockchain can only compete with those registry systems functioning merely as document archives. In more legally advanced registration systems such as those in Germany or Spain, where protection of the registering owner depends on the validity of the registered acts and transactions, blockchain can serve as little more than an additional form of presenting documentation for Property, Business and Chattel Registries.

Although the opposite may seem true to laymen of computer science, blockchain is not a revolution, but rather a simple evolution of several technologies that have been present in our daily life (often invisibly) for many years—from the use of peer to peer networks to distribute files to asymmetric key cryptography to encrypt their content.

It is simply a matter of assigning a unique alphanumeric code to a file when it is created, in such a way that any modification introduced to it, however minimal, will give rise to a different code, documenting the change. Since one of the attributes generated by that code is the date the file was created (or modified), there would be no doubt as to when the transaction was made, whether the file in question was a contract, or its content (which cannot be altered).

The reader versed in IT will immediately see that all this has been possible for a long time through mechanisms such as electronic signature. Blockchain is nothing more than the reuse, in a different format, of a set of technologies that have been in use in registry systems like Spain's for more than fifteen years.

What then are the advantages of blockchain for a system that already has what it offers? In terms of Registry, none. All the benefits of blockchain applied to contracts actually affect the notarial sphere, insofar as the files generated by blockchain can render the traditional distinction between public and private documents obsolete, as there is evidence of the date of signing, the integrity of the document and even the identity of the parties.

On the other hand, for Property, Business or Chattel Registries, the use of the blockchain not only brings no added value (since all its benefits exist and have been used for years), but paradoxically, highlights the system's limitations when applied to a public record rather than a database.

The first practical drawback is that a registry system that assumes the blockchain with all its consequences would have to automatically leave out all non-electronic contracts. This is equivalent to preventing access to millions of existing property titles. Because either these titles will continue to

be able to access the Land Registry under the same conditions as electronic documents (which is the system in countries such as Spain), in which case the novelty disappears immediately; or only electronic documents have access to the registry and those that are not electronic must be granted again, in which case the law that recognizes their legal effectiveness would be without object.

It is no coincidence that countries in which block-based registry systems have been implanted have little or no registry tradition. In these systems, property rights are seldom recorded, and there is no other solution than to periodically redistribute the land by graceful concession of successive rulers, precisely because of the impossibility of the owners to prove their right. Creating ex novo an electronic record in such countries poses no problem because non-electronic titles either do not exist or would not have been registered anyway.

But the question is very different in countries with greater legal and economic stability. If millions of non-electronic proprietary titles are left out of the system, the alleged cost reduction disappears immediately, because then there would be a need to deal with litigation over property rights in courts of law.

The second limitation of a registry system based on blockchain is rarely considered because its supporters are computer scientists, not lawyers, who tend to confuse public records with databases.

In a database, the administrator's responsibility extends only so far as to assure that the data contained in the database is correct. But in a legal registry, the registrar is also responsible for the validity of that data, in other words, its compliance with the law.

A database, however sophisticated its metadata may be, is merely a list of the people or goods that appear in it. But in a legal registry, these data are property rights, recognized by the State as binding for third parties who no longer hold right to ownership. Ownership is now limited to the registered owner. In a database, an incorrect owner listing is an error; in a property registry, an erroneous inscription in favor of a party who did not legally acquire a property is equivalent to depriving someone of their property rights.

This confusion between registries and databases is to a certain extent understandable because in the weaker registries of comparative law, the Registry of Ownership functions as a mere archive of documents. In them, registration is based on priority and sequence principle, which are determined by objective data (the date and time when the document was presented, or the identity of the transferring registrant). It is conceivable that such circumstances could be assimilated to the metadata of an electronic file, and therefore routinely interpreted by blockchain supporters.

However, in those countries where the Land Registry operates as a register of rights, registration is not a simple way of reconstructing the transmission chain (which is what the blockchain, by its own mechanism, tries to accredit), but the legal basis for a whole series of presumptions in favor of the owner, even going so far as to make its acquisition unattainable by the courts of justice if it meets the requirements established by law.

These assumptions rest on the Registrar's qualification to validate the rights of those registering property, not only in form but in substance—a function that blockchain, due to its purely technological nature, is unable to perform.

When this limitation became evident, the solution proposed was the use of so-called smart contracts or intelligent contracts together with blockchain, in that they would access the contract forms registry.

But we encounter many difficulties when we insist on applying database solutions to a legal register. The first is freedom to contract, as database solutions would require contracting parties to adhere to existing forms. In this case, either the forms will be extremely simple, suitable only for the simplest transactions, or they will be excessively cumbersome if they are intended to cover all possible eventualities, immediately eliminating the alleged reduction of transaction costs.

And yet, when compared to a legal record based on qualification, the combination of blockchain together with smart contracts continues to prove insufficient for several reasons. For one, the Land Registry can access acts or business dealings from around the world, provided they are valid. But not even the most meticulous of smart contracts can contain all the world's legal systems in its clauses because the rules and Jurisprudence of different systems are often contradictory.

Second, contracts, by their very nature, only produce effects between the parties, whereas the characteristic of property rights is that they produce effects against third parties. The fact that a contract produces not only obligations but real rights, whose ownership is exclusive and excluding, no matter how long, may encompass. This is because the binding effect for third parties depends on consent that they provide neither at the signing of the contract nor at a later date (Pre-existing Real rights, legal domain limitations, judicial and administrative decisions, etc.) that neither are nor can be part of the content of a contract, but are nevertheless essential for the contracting party to become the owner.

And that is why no "intelligent contracting" system can replace a Land Registry, especially if it is a register of rights (based on the qualification of the form and the background of the titles), because not only the contracts have access to registration, but also a whole

series of non-contractual acts of a judicial and administrative nature that decisively influence the realm and other real rights: embargoes, prohibitions to dispose, competition of creditors, incapacitation, delinks, urban planning actions, etc.

Of course, all these judicial and administrative documents may also have access to the Land Registry in electronic format, as they have for years. This is because a well-established registry system uses technology to operate more efficiently.

But this is a different question from the intention to restructure an entire legal system dedicated to the protection of the right of ownership only to accommodate technology that neither offers substantial progress in the operation of existing registries nor provides more guarantees for the owners of property rights.

The Blockchain Cures Cancer (and replaces notaries, etc.)

Matt Regan, CEO
Epigraph, Austin, TX (USA)

Spoiler alert: Blockchain has not cured cancer, nor is it reasonable to suggest that it will, by itself, cure cancer or solve any number of other "big" problems with which mankind presently struggles. Blockchain is a tool, not a panacea. It is a powerful technology that, when carefully applied to real world problems as part of a well-conceived solution, may move the needle collectively forward in a number of arenas. So, what does this have to do with land registration and notaries? Technology has offered a way to improve the quality and reliability of land registries, but it is up to the people who are responsible for, and interact with these registries, to take advantage of this opportunity.

A few years ago, some forward-thinking people began to hypothesize on how a new and exciting technology might be used in innovative ways to solve long-standing social, economic, governmental and technical challenges. That technology was blockchain, a distributed ledgering system that promises data immutability – a feature that truly could have the power to solve real and age-old challenges. Until that point blockchain was being used exclusively as the backbone underlying

Bitcoin, the mostly infamous, but very real and valuable, digital currency; but problem solvers looked beyond Bitcoin and saw what the promise of immutable, trustworthy data could bring to software application design.

Fast forward to present day, and most everyone in the land registration community has at least heard or read the term "blockchain" – and in some cases, may even have some level of understanding as to how the technology actually works. Land Registration was tagged as an early use case for demonstrating the power of blockchain, and as a result the lines quickly blurred between "what could be" and "where we are today" as blockchain evangelists who were eager for real world applications latched onto any potential breakthrough that would anoint blockchain as "having arrived." In reality, while several places and groups of people are pushing to see blockchain used in land registration, we are still waiting for "meaningful use" and may realistically be waiting for a while longer.

Is this all to say that blockchain technology has no potential to change how land records are secured? Not at all. If you gain a quick understanding of blockchain and know something about land registries, you will more than likely become convinced there is something to the thought that blockchain could vastly improve the systems currently in place throughout much of the world. What this all means is that now is the time we should be learning about blockchain, developing some basic understanding of the underlying principles, and thinking about (and preparing for) how it may change the status quo.

Blockchain 101

The first order of business then, is to develop some basic understanding of blockchain technology so that we can intelligently think about how we in the land registration community can use it to do our job better.

To understand the blockchain it is best to begin with why it was invented in the first place: Bitcoin. Bitcoin is an electronic payment system based on cryptographic proof, which allows any two willing parties to transact directly without the need for a trusted third party (traditionally "the state" or a bank) to guarantee the value of the payment. In theory, digital assets are especially susceptible to "double-spending" or counterfeiting, due to the ease with which they can be manipulated. However, transactions that are computationally and logistically impractical to reverse protect participating parties from fraud. Bitcoin presents a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.[1] This proof is what guarantees that the Bitcoin being exchanged belongs to the grantor, and is available to be transferred

[1] *Nakamoto, Satoshi. (2008). Bitcoin: a peertopeer electronic cash system. Retrieved December 28, 2015, from https://bitcoin.org/bitcoin.pdf*

to the grantee, at the exact moment in time in which the transaction occurs.

The technology underpinning the digital currency—commonly called "the blockchain" or "blockchain"—is considered the main technological innovation of Bitcoin. The blockchain is a public ledger of all Bitcoin transactions that have ever been executed. The blockchain is constantly growing as "completed" blocks are added to it with each new set of transactions. The blocks are added in a linear, chronological order. Each node (computer connected to the Bitcoin network running software that performs the task of validating and relaying transactions) maintains a copy of the blockchain. New blocks can only be added to the blockchain once a majority of nodes perform, and agree upon the solution to, complex cryptographic proofs. The blockchain contains complete information about every Bitcoin transaction from the genesis block to the most recently completed block.[2] The distributed design of the blockchain (also known as a distributed ledger), maintained across thousands of independent nodes, makes it effectively impossible to hack and alter. A malicious actor would have to change every copy of the ledger on a majority of the network nodes to alter the history of the ledger. The result: immutable data that can be reliably read, or one could say audited, from any node in the network. This is the power of blockchain.

While Bitcoin is the first functioning example of blockchain technology, it does not represent the only blockchain. The concepts of blockchain can be used by any network of computer nodes that are organized to work together in the task of creating and sharing an immutable dataset. New blockchain based networks are introduced almost daily—to the point where it is difficult to keep track of them or predict which will have staying power. Bitcoin's blockchain remains the most well-known, and because of the value of Bitcoin, arguably the most reliable. Bitcoin's blockchain was not designed to store data beyond the asset transactions themselves, however, so new blockchains that are built with data storage in mind are sure to gain traction and become reliable tools for creating and maintaining immutable data.

Sit up, walk ... run, jump

Blockchain is a compelling tool. When considered in the context of land registries, and the challenges that land registries historically face, especially in developing countries, the possibilities for improvement are exciting and manyfold. Does this mean that starting tomorrow we should turn to representing all property rights as blockchain tokens exchanged via smart contracts that require no human oversight? Easy question, the answer is no.

By acknowledging that blockchain technology is interesting and worth

2 Blockchain. n.d. In Investopedia. Retrieved December 28, 2015, from www.investopedia.com/terms/b/blockchain.asp.

considering, we are "sitting up." This is an important first step. Let the next step be "learning to walk." Only once we are walking with confidence should we consider "running" and "jumping." Property rights are a very serious matter. They are a core element of the foundation on which liberty, society and economies are built. They should be treated with due respect.

It is exactly this respect for the importance of property rights that compels us to use the immutability and auditability of blockchain to protect property rights in ways we are not doing today. "Walking," in the context of adopting blockchain in land registries, can mean incorporating blockchain into existing practices in order to improve those practices and the records that they produce. Developed countries may take for granted that instruments will not be intentionally or accidentally altered during or after the recording process, but the developing world is afforded no such luxury.

Blockchain provides us with an immediate solution to this problem via its immutability. There is a better approach than placing newly drafted instruments in manila folders that countless workers touch prior to recording. There is a better approach than recording these instruments in paper books, or centrally housed databases, where nefarious actors can make untracked changes to "official, final" versions. Without major disruptions to existing recording processes, we can safely record new instruments simultaneously on a blockchain, ensuring that once recorded these instruments are never modified. This represents a real, measurable improvement—and effectively zero risk. This could take the form of a new land registry application that replaces an outdated solution, or could simply be tacked onto an existing solution as a parallel process.

Value added, low risk.

What other low hanging fruit undermines the reliability of many land registries around the globe? Transparency. As property rights are highly valuable, and instruments are presently at risk of being altered, recordings must be carefully protected. Combine this situation with the corruption that can exist within land registries and it creates a trust problem. Blockchain's immutability and decentralized nature combine to offer a solution to the transparency problem. Instruments recorded in the blockchain will be immutable, meaning tamper-proof. The record of each instrument can also be made accessible (if desired) via every node in the blockchain network, meaning they are thus auditable by anyone that wants to make sure the land registry is doing what it is tasked to do without risk that these auditors can modify the instruments.

Suddenly, people know what is being recorded, and can be assured the records will not change. To be clear, this only introduces a new level of precision in land registration,

but it does not, on its own, ensure accuracy. It does however lay the groundwork to a gradual improvement in the accuracy and quality of land registries as notaries, courts and other land title professionals are no longer asked to base their decisions on a moving target. Over time, as these improvements in accuracy accrue, we could see the real value of recording instruments into the blockchain as economies built on enforceable property rights are allowed to mature.

The role of the notary in this process remains absolutely critical. There is an old saying in the computer profession, "Garbage in, Garbage out." This warning is worth heeding as we look to record instruments into an immutable data store. While there has always been, and will continue to be, corrective measures available to cure title imperfections, it is always the goal to create instruments that are as correct as possible. The blockchain does not solve this challenge. That challenge will continue to be the job of the notary who creates these instruments that define and transfer property rights and ensure the parties involved in the transaction are who they say they are. The blockchain solidifies and protects this quality work product produced by the notary.

As time passes, and a critical mass of instruments are safely recorded using blockchain, the land registration community can look to further improve its data and services by taking advantage of the blockchain and other upcoming tools, whatever they may be at the time. This is the natural progression of technology. Following that progression makes sense, but we must start at the beginning, not from the middle.

Let's get started

As with any new technology, a measured dose of skepticism and pause is a natural and healthy reaction. The next step however, is to cut through the hype and do the work required to safely determine if this new tool, blockchain, will improve the work we do. In engineering this is called a proof of concept. Immutable and auditable land registries, designed to protect property rights, is a concept difficult to argue against. Why not get to work to prove its feasibility?

The Impact of "Disruptive" IT and the Registrar's Role in Future e-Conveyancing

Jacques Vos, Land Registrar
The Netherlands

Abstract This paper is about the functioning of blockchain technology and the possible use or impact it may have on current Land Registry systems. It is concluded that "disruptive" techniques can be helpful in many cases, as long as they do not compromise a system of checks and balances. Although lawyers should make use of modern techniques in becoming more inventive solution thinkers, it is clear that Land Registers are too important to be replaced by a technique that is not suitable or does not yet fit the needs of the public. The study included developments leading up to January, 15, 2016 and therefore does not describe or comment on more recent developments.

Blockchain

Blockchain is a technological solution to register transactions without the services of a trusted third party. It is a type of consensus-based computing that facilitates Bitcoin and other services. It is often said that banks, governmental parties, Chambers of Commerce and Land Registry authorities should keep an eye on blockchain. It is even said that these parties may be challenged—or even replaced—by this, what has been sometimes referred to as "disruptive technology". Analogies have been made between blockchain and the old paper process as a ledger. It is a method of recording data—a digital ledger of transactions, agreements, contracts—anything which needs to be independently recorded and verified

as having happened.[1] It is a record of who owns what at a certain time. It keeps track of transactions, it documents when a transaction took place and it ensures that there is always one single owner and no double usage of the same item or unit.

Based on its characteristics, (shared database, multiple writers, no intermediation, transparency, timestamping, transaction rules and validation) blockchain truly seems to be an ideal and unique functioning system. However, it is still not certain that this technology could be used in diverse cases or that it could run a land registry system.

It is known that the number of Bitcoins is limited to twenty-one million. Each Bitcoin contains one million units (bits) and each bit is separately identifiable and programmable. This means that every unit can be given specific properties. Therefore, it is possible in theory to use blockchain technology for trading in Eurocents, in shares of companies, in Kilowatts of energy or in votes in an election. It is also possible to 'smarten' these specific units (e.g.: to employ the vote during elections for 2016 or to pay with the bits only for repaying tax debts). In such cases, compliance would not be verified afterwards, but rather would be programmed into the units and the system itself, meaning that compliance could be checked for in advance. It is also possible to program the units to automatically return to the issuing authority in case the unit is not used or to earmark the unit (e.g. in case a grant is awarded or taxes have to be paid), potentially saving on many overhead costs. The programmable and open nature of blockchain makes is possible to rebuild or innovate financial or administrative processes.

Trust: indispensable for Land Registry

A Land Registry system is successful when all partners involved (owners, banks, Notaries, etc.) have trust in the system. This is independent of legal and technical solutions. Having trust means that a third dimension including the organizational or institutional aspects of the system must be taken into account.

In some (usually developing) countries, people do not always trust the current Land Registry system. In some cases, systems are fraught with fraud and corruption and in other cases, there is merely a lack of quality. A blockchain-based Land Registry system may appear to bring a solution to these problems, but in reality, it might not. The real challenge in these countries will most likely be the initial and definitive identification of those holding rights to properties and the creation of actual titles. Once the actual owner of a certain parcel has been determined, the ownership of the parcel can be transferred. But this initial phase will not be carried out by using blockchain. Blockchain is designed as a 'shared single source of trust',

[1] *http://www.bbc.com/news/business-35370304 (Last accessed on January 15., 2016).*

to exclude mistrusted governmental parties and banks, but it requires an empty stage upon which all parties can agree as a starting point. This Genesis block will be the problem in the case of certain countries, because there is no trust in the system and therefore no consent among the interested parties. In such cases, a blockchain-based Land Registry will not work.

The use of blockchain in Land Registries

The functionality of blockchain can be described as a digital ledger. It serves (more or less) the same functionalities as a sound Land Registry system: it knows who owns what at a certain time, it ensures single-ownership and it knows when transactions took place. It is possible to 'track back' and therefore should be possible to guarantee title.

Compared with a "classic" land registry system, blockchain may even provide some additional certainty because of the techniques used. Because of its transaction dependency, in a blockchain, it is not possible for a non-owner to transfer ownership. Checks on ownership using blockchain technology are processed automatically, using transaction dependency and transaction rules, whereas in current Land Registry systems checks on ownership are executed by the Registrar, mostly by scrutinizing the deed and comparing this information to the content of the land register in person. This means that in most cases, the data of the seller mentioned in the deed is compared in person to the data of the current owner in the land register, although there are other existing technological solutions to prevent manual processing of data and checks.

The content of a blockchain is public (except when a private or hybrid blockchain is used). It cannot be changed, as recording of the data is time-stamped and multiplied and therefore indisputable. In current Land Registry systems, this is applied by using time-stamps and audit trails.

The principles of Land Registration are often divided into four parts: the specialty principle, the booking principle, the consent principle and the principle of publicity. In the registration of Anglo-Saxon titles there are three fundamental principles: the mirror principle, the curtain principle and the insurance principle. Some of the demands of these principles are met by blockchain technology, but some are certainly not.

With regard to Governance of a blockchain-based Land Registry, it is questionable who would design and keep the Land Registry data. In relation to this question, it is of great importance to determine whether the Land Registry should be kept in a private, a public or a hybrid blockchain.

To introduce a Land Registry blockchain in a country with a well-developed Land Registry system, it would be necessary to

know and incorporate all existing *in rem* rights and all existing Land Registry objects in the first block, the Genesis block. If not all *in rem* rights and objects are incorporated in the system, there is no way to represent the actual situation with regard to the objects and *in rem* rights concerning all immovable objects.

The use of so-called sidechains may be of help to divide a parcel (a parent chain) into a set of apartment rights (a sidechain). It would also make it possible to move the object in the sidechain (apartment right) back to the parent chain (parcel), for example in the case when an apartment building may be restructured or a usufruct or lease may end under specific circumstances (for example, death or passing of a period of time).

In a country where there is no *numerus clausus*, the introduction of a Land Registry blockchain might even be more complex. In such a system, new rights *in rem* can be created. Those specific rights should then perhaps be put in another sidechain. Another possibility might be the possibility to smarten specific units within the blockchain by adding a certain value or meaning to a part of the asset.

Actual and complete information

There must be some form of consensus about the content of the Genesis block. This means that, in the case of a public Land Registry blockchain used by everyone (and not solely by Registrars and other professional parties), there should be consensus on the actual situation. In creating the Genesis block, existing and well-functioning title systems and Torren`s-based Land Registry systems seem to be the most appropriate for using blockchain technology. In the case that such a Land Registry system is not complete—in many countries there are still first entries to be made—the blockchain may be less suitable. In such cases, it could only be used for the registered parts of the parcels and objects. Unregistered properties cannot be put in the Genesis block.

There is a risk of presenting information that does not represent current information. This can be the case during the mining process. These so-called "Proof of Work" or "Proof of Stake" consensus models may take up to ten minutes' time.

During these waiting periods, the assets are locked. This would block the conveying of immovable assets for a certain period of time, especially in a situation that is called a 'fork', while in a 'classical' Real Estate system the deeds are received and traceable, if not published immediately. This is why in most Land Registry systems it is possible to transfer ownership multiple times in a short period of time, still being able to investigate the actual (legal) situation.

Easy to understand

Most "classic" Land Registry systems utilize an ABC-structure, containing all

information about the object, the subjects involved, the most embracing right *in rem* (mostly ownership) and the applicable other rights *in rem*, burdens and easements. In a Blockchain system, this brief overview or ABC-structure may be more complex to carry out, as it will use sidechains, especially in situations where a 'bundle of rights'[2] —and therefore multiple sidechains—is applicable. Data retrieval, using several search entries to conduct legal research on a subject or an object, are elements that blockchain technology does not yet provide.

Blockchain will not change a legal system

A Land Registry system cannot be changed from a deed to a title or Torrens-based system or vice versa by introducing a blockchain-based Land Registry. It will not bring any changes to any system. What goes in will come out. In the case that blockchain is used in a deeds system, a title will still not be issued by the Registrar. In the case of a title system, the title will be transferred by using blockchain; the title will not get lost.

Blockchain technology will not improve legal certainty regarding the content and legal meaning of the first block. In a case where there is uncertainty as to the title holder,[3] blockchain will not bring any changes to this level of certainty. Improving quality and completing Land Registers can possibly be carried out by recording new transactions and/or—depending on the legal system—adding titles in the subsequent blocks or by uploading new transactions to the first block.

Preconditions and exotic transactions

In many cases, pre-existing conditions exist that are of importance in the process of transferring ownership. It could be a spouse or co-owner who must give consent for the selling of marital property, the dissolving condition of funding or any other precondition the parties have agreed upon (transferring ownership, free of mortgages, seizures and other burdens). Conveying property rights starts with identifying the parties involved. In a situation (or a country) where citizens do not have reliable electronic identities, this will be the first problem to solve. In a "classic" Land Registry system it is the task of both the licensed conveyancer/ Notary/Surveyor and/or the Registrar to check identities and to determine whether the preconditions have been elaborated or not. In a blockchain system, the deed will not be scrutinized by a person, but rather by the system itself. In order for this to work, smart contracts infrastructure may be utilized, consisting of computer protocols that facilitate, verify or enforce the negotiation or performance of a contract, or that obviate the need for a contractual clause. Since 2008, so-called stylesheets have been used in the Dutch Land Registry system to scrutinize deeds, carry

---

2 The 'bundle of rights' is a common way to explain the complexities of property ownership. It is commonly taught in Common Law systems.

3 eg. prescription cases that are not registered, disputes on boundaries and deceased persons where the heirs did not register a certificate of inheritance.

out checks and requirements for registration purposes and to a certain extent check if specific conditions are met. These tasks are carried out in a different way, but with the same result. One might say that these stylesheets are also smart contracts (the code, with certain preconditions, to transfer ownership).

Conclusions

In conclusion, as transaction rules can be implemented, the validity of transactions can be checked. In current Land Registry systems, this is mostly executed manually by scrutinizing the deed. In some cases, this can be done by computers, as is the case in stylesheet-based deeds. The business rules incorporated in the stylesheet can be relatively similar to the transaction rules in smart contracts which can be used in blockchain technology.

Therefore, we may conclude that in the case that a Registrar is planning to introduce automated deed processing, blockchain could be one of the technologies utilized. However, further research is needed to ensure that this is possible.

In the case that a blockchain-based Land Registry system is implemented, one should not underestimate the complexity of the legal system, the meaning of the *in rem* rights (*numerus clausus* or not), the complexity and variety of diverse transactions and the proceedings of legal professionals in the chain of conveying immovable property.

This complexity would increase if a cross-border Land Registry blockchain were introduced because there should be an empty stage which everyone can agree on. This empty stage would mean the objects are known and registered, the various *in rem* rights are known and registered and there is an agreement on differences between common law and civil law principles and causal and abstract systems.

Sometimes technology professionals and other enthusiastic decision makers express their opinion that modern technology solutions can replace legal professionals quite easily. Without the cooperation of legal professionals, who indicate the legal meaning and its implications, these technologies will not be applicable in the right way. Implementation of such technology would result in pure chaos.

Implementing blockchain technology would mean reliance on the legal expertise of professionals in the field of electronic conveyancing. For the drafting of deeds, this person is the licensed conveyancer or the Notary and for updating the Land Register it is the Registrar.

Assuring legal knowledge for attorneys in the future, including legal professionals from the "classic generation" means it is time to shake hands with the "disruptive generation", and the new technological solutions it is creating. Whether legal proceedings and checks are executed by a computerized system or by hand, it is important that liability

has been covered. It is also important that someone is able to solve problems in the case that something goes wrong. The role of lawyers is not expected to be completely replaced by “disruptive” technologies. People rely on technology but want to be able to refer to a lawyer in case of problems. As lawyers should make use of new—and trustworthy—technology as much as possible, they should work closely together with technology developers.

BOOK REVIEW
Das Grundbuch im Europa des 21. Jahrhunderts [Land Registry in 21st Century Europe]

Arkadiusz Wudarski (ed.)

Duncker & Humblot, Berlin, (Germany) 2016, 783 pp.

It may not be too bold to say that the first wave toward the unification of European Civil Law focused on Contract Law has passed, broken against the breakwater of national legal systems; and to say that now, in a time of certain instability, the unifying movement is exploring new areas before considering its next step.

Property Law seems to be a focal point among these areas. As Kieninger has said, if Property rights were treated until recently as the half-brother in the harmonization process, they are now called to occupy the center of the scene in coming years (Kieninger, "Perspektiven fürein Europäisches Mobiliarsicherungsrecht", ZEuP, 2016-1, p. 201). And Land Registry will play an important role.

This text is a good example of the new focus. It is result of an international research project entitled "Functions of Land Registries in European Comparative Perspective", carried out by Arkadius Wudarsky, Chair of Polish and European Private Law and Comparative Law at

the Frankfurt (Oder) University, in cooperation with two other Research Groups. The volume comprises twenty-seven chapters and the work of twenty-eight researchers—some as co-authors, some collaborating on more than one chapter. It includes studies about different aspects of Land Registry Law from Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, the Czech Republic, England, France, Germany, Greece, Ireland, Italy, Poland, Romania, Scotland, Spain and Switzerland. Most of the papers (18) are written in German, and the remaining 9 are in English.

The book primarily involves comparative analyses of various Land Registry systems, focusing especially on their protective functions. But the authors also deal with a number of other subjects such as personal data protection, registration of personal rights and the role of possession, among others. At times the authors' perspectives seem not to be in exact accordance with one another because issues are dealt with in one country but not another, but such differences can be expected in collective works.

The volume is divided into five sections. The first focuses on the registry as part of the legal system, and is composed of five articles. The first, written by the book's editor, Arkadiusz Wudarsky, deals in general with the concept of land registry and its placement among different types of registries (private and public registries, administrative and juristic ones, with positive or negative effects). In the second article, Peter Mankowski looks at the problems of private international Law relating to land registry. The three remaining papers in the first section of the book address general problems from national points of view: the relation between the German system of property rights and its land registry, focusing on the role of notaries (Stefan Hügel); the registry and its function of curing blemishes in titles in the English system, including an interesting exposition of the history of English land registry Law (Simon A. Cooper); and the combination of contractual freedom and registration requirements in the acquisition of real estate in Austria (Peter Bydlinski).

The second section of the book, about the contents of the land registry and its settings, is also composed of five chapters. In the first, Artur Barańsky and Arkadius Wudarski address the role of the registry as an instrument to grant effect against a third party to personal rights. The second deals with prospect rights and their possible registration in German and Polish Law. In the third, Mark Jordan focuses on the differences between the English registry system and the German model, emphasising the function of possession and also partial indefeasibility in the English system. The fourth article offers Tatjana Josipović's general description of Croatian registry, with constitutive registration and public faith, inherited from

Austrian Law. The fifth and final paper in the second section of the book studies a partial aspect of Italian registry which allows for the inscription of preliminary contracts (Riccardo Omodei Salè).

The third section of the book addresses the principle of public faith in registration, and six authors focus on this subject within their respective legal systems. Romana Cierpíał-Magnor and Arkadius Wudarsky explain the Austrian System and the conditions which must be fulfilled for an acquisition to be protected by the registry (acquisition based on an onerous legal act). Eva Dubrovolná and Artur Barańsky describe the Czech system, very similar to the Austrian, which was its model and which it once again more closely resembles since the fall of communism. Javier Gómez-Galligo presents a synthesis of the Spanish land registry, placing it within the general framework of the various registry systems, and emphasizing the principles of Spanish Land Registry Law. Emma Lee in turn offers an exposition and strong synthesis of the English and Welsh Land Registration Act of 2002, focusing on its protective function, and the different kinds of errors the Registry can contain. Kenneth G. C. Reid presents Scotland's new Land Registration Act of 2012, which in part is an attempt to find a balance between a Registry of deeds and the protection of purchasers. Finally, Vincent Sargent describes the Belgian registry system, characterized by the merely negative effects of registration, which have gone uncorrected by any of the mechanisms introduced in other countries following the same principles.

The book's fourth section looks at Registry's transformations throughout history. It contains a more general chapter about the development of the Registry in Europe from its Origins to the present, written by Werner Ogris, Arkadiusz Wudarsky and Artur Barańsky. Although it focuses on central Europe, the article is a masterful piece of work. The five other papers dealt with particular aspects of the evolution of the land Registry in Romania (Eugen Chelaru), Austria (Gerald Kohl), Bosnia and Herzegovina (Meliha Povlakić), Cyprus (Tatiana-Eleni Synodinou) and Poland (again by Arkadiusz Wudarski).

The fifth and last section, entitled Challenges to the Registry Today, is composed of five articles. The first, written by Julien Dubarry, explains some internal relations between the principles of French Property Law and its registry principles, such as the coordination of consensual transfer of property and not constitutive registration. Dubarry concludes from his study that it would be difficult to create a single land registry in Europe, precisely because it depends on the system of property Law in each nation. The second chapter, written by Ioannis Papadimopoulos, offers a general description of the Land Registry in Greece. In

the third chapter, Luz M. Martínez Velencoso analyzes some of the most problematic aspects of Spanish Land Registry, such as the role of possession, data protection or the function of the Registrar. Harald Wilsch dealt then with the computerization of the Registry in Germany and the problems electronic commerce has been provoking. The book ends with a chapter by Stephan Wolf and Jonas Mangisch on the Swiss registry system, organized according to the principles by which it is governed.

The book is full of information and is very enriching for any specialist in Land Registry Law. Obviously, as in any collective work, some chapters are more interesting than others—also, due to the reader's own interest in some subjects—; but the general level of the work is of excellent quality. In fact, in my view, beyond the fact that some European land registry systems were not discussed, probably because suitable authors were not found for those countries (Holland, Portugal or the Scandinavian countries, among others), the only criticism that can be directed at the book is its structure, because the reader sometimes has the impression that the classification into sections is somewhat artificial or forced. Some chapters could be in one section or another without a clear criterion. Perhaps, in that sense, it would have been clearer to divide the book into papers on general questions relating to all legal systems, studies on the registry of each country and papers on more specific issues. In any case, these are matters of opinion and do not diminish in any way the value of the volume.

Bruno Rodríguez-Rosado
Universidad de Málaga, Málaga (Spain)

ipra-cinder
INTERNATIONAL PROPERTY REGISTRIES ASSOCIATION

IRIB
Instituto de Registro
Imobiliário do Brasil

ABDRI
ACADEMIA
BRASILEIRA
DE DIREITO
REGISTRAL
IMOBILIÁRIO

Quinta
editorial